Zero Trust

The Concept, Standards, Requirements, Timeline, Directions

Dennis Moreau,
Sr Engineering Architect, Cybersecurity
VMware, Research and Innovation, Office of the CTO

9/24/2021

Agenda

What is Zero Trust and how does it work (to address supply chain security, ransomware and complexity)?

Where are the standards now?

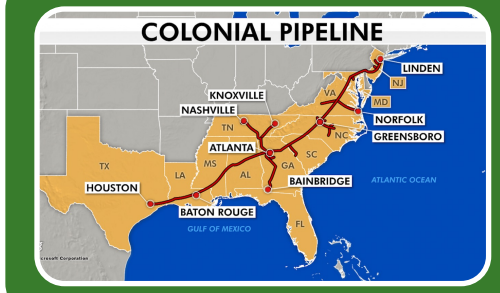
- NIST ZT Reference Architecture
- DoD ZT Reference Architecture
- NIST Guidance on ZT for Microservices and Service Mesh
- NCCoE Collaboration on ZT

The ZT Timeline

Guidance

- NIST NCCoE Audit Guidance
- CISA Maturity Model
- CISA Cloud security Reference Architecture
- Timeline (EO-14028, CMMC, EU NIS2, …)
- UK NCSC ZT Architecture Guidelines
- EU NIS2 ZT (ENISA) – Parliament vote in November

ZT Assumption of Compromise == Supply Chain Attack.

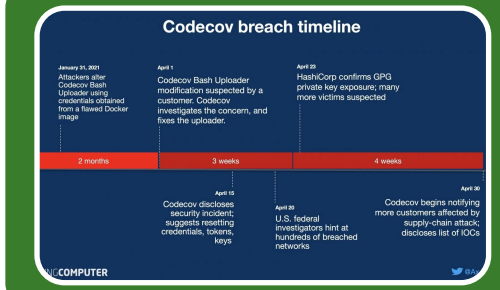


Colonial Pipeline RW & Exfil Attack (DoubleDip)

- 5000 Mile Pipeline, 100s of Remote Valves, 200 Mft^3, $5M Ransom, $$$ Business Impact…
- 400,000 Pipeline mile potentially vulnerable. $$$$ Threat is orders of magnitude larger in just pipeline control, availability, safety
- $$$$$ Remediation – eDesign, Replacement , OpEx++, Reg, …

SunBurst (Solarigate) Supply Chain Attack

- Undetected for 15 Months (despite 18K Security Portfolios & Teams)
- Injected into the DevOps cycle, Global Sourcing (Bulgaria), Inadequate curation/testing/isolation …
- Triggering standards, regulatory and procurement response (see WH EO)



CodeCov Supply Chain Attack

- Any credentials, tokens, or keys passed to Continuous Integration runner
- Any services, data stores, and application code that could be accessed with these credentials, tokens, or keys
- 19,000 Customers including IBM, HP, Atlassian, Rapid 7 … who are also participants in supply

Long Undetected Compromises, a Prelude to Many Ransomware .

Supply Chain [1]

- Attacks up by 42% in Q1 of 2021 – Data compromise only increased by 12%
- Q1 SC Attacks: 27 Vendors, 140 Organizations publicly reported as targets, 7.4 M impacted
- Number of affected individuals up by 560%
- Trend is to compromise multiple organizations through one point of attack
- Huge spike in insurance claims due to services outages (MS Exchange Attack 30,000-60,000 Orgs) – Legal, Forensic , Cleanup, Disruption and Fines

Increasingly Combined with Data Extortion (ransomware) [2]

- 228 Industrials and Engineering
- 225 Manufacturing
- 145 Technology
- 142 Retail
- 95 Healthcare

Pressure is on governments to “Do Something”!

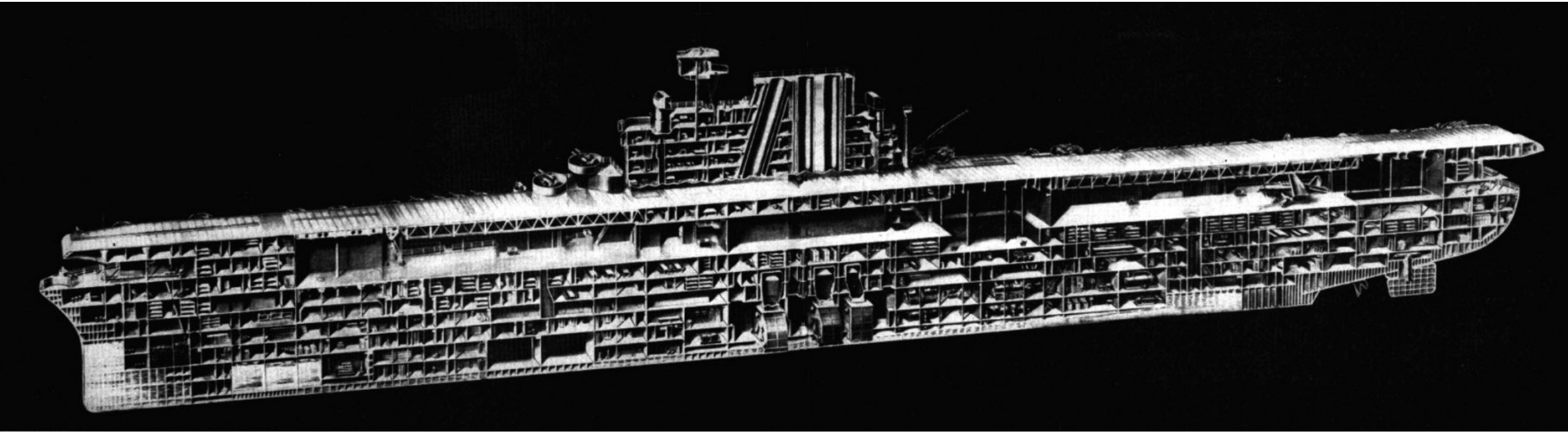
Enter the EO for Improving National Cybersecurity, NIST, CISA, NSA and the DoD…

Sources (1) Crowdstrike 2021 Global Threat Report

(2) Identity Theft Resource Center 2021

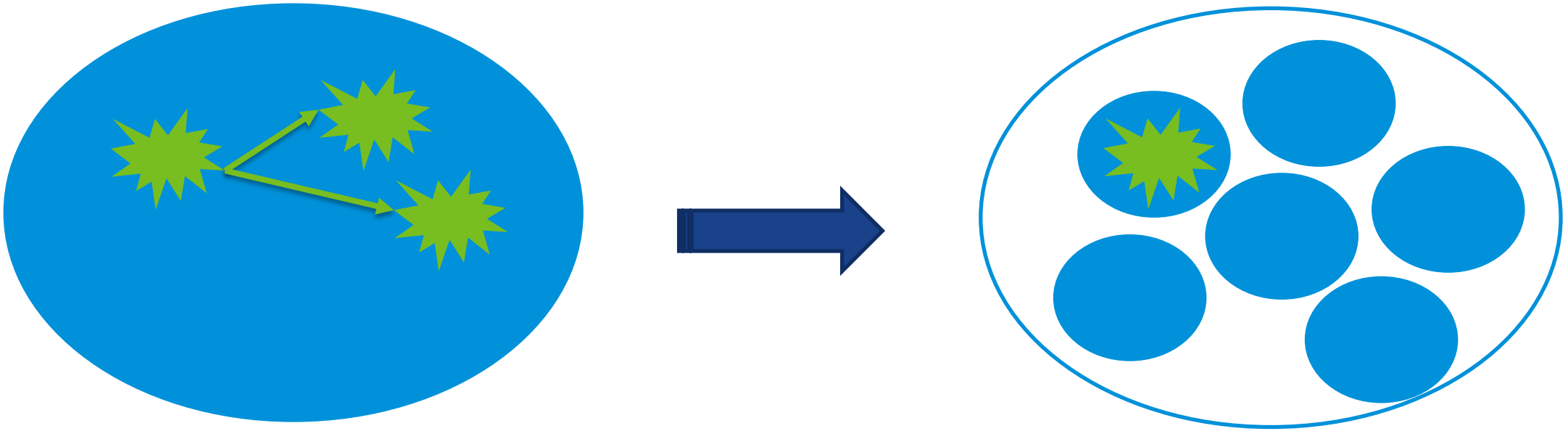
Zero Trust – is a very different policy approach …

Continuous, Granular, Policy Enforcement & Containment …
… via Compartmentalization (by application/service)



ZT Requires that we Assume Compromise … soooo

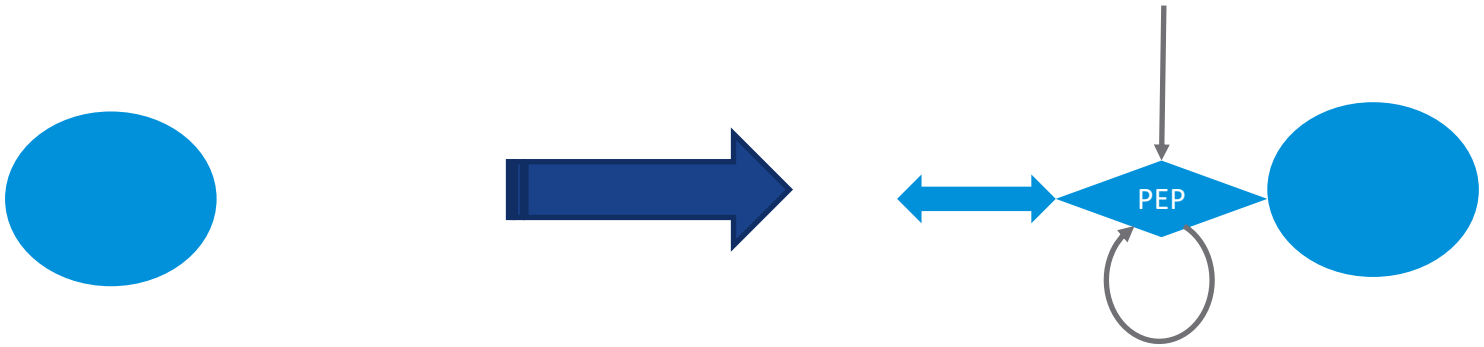
ZT Assumes compromise in supply chain and in the perimeter … so, compartmentalization is necessary.



But complete compartmentalization is not very useful …soooo

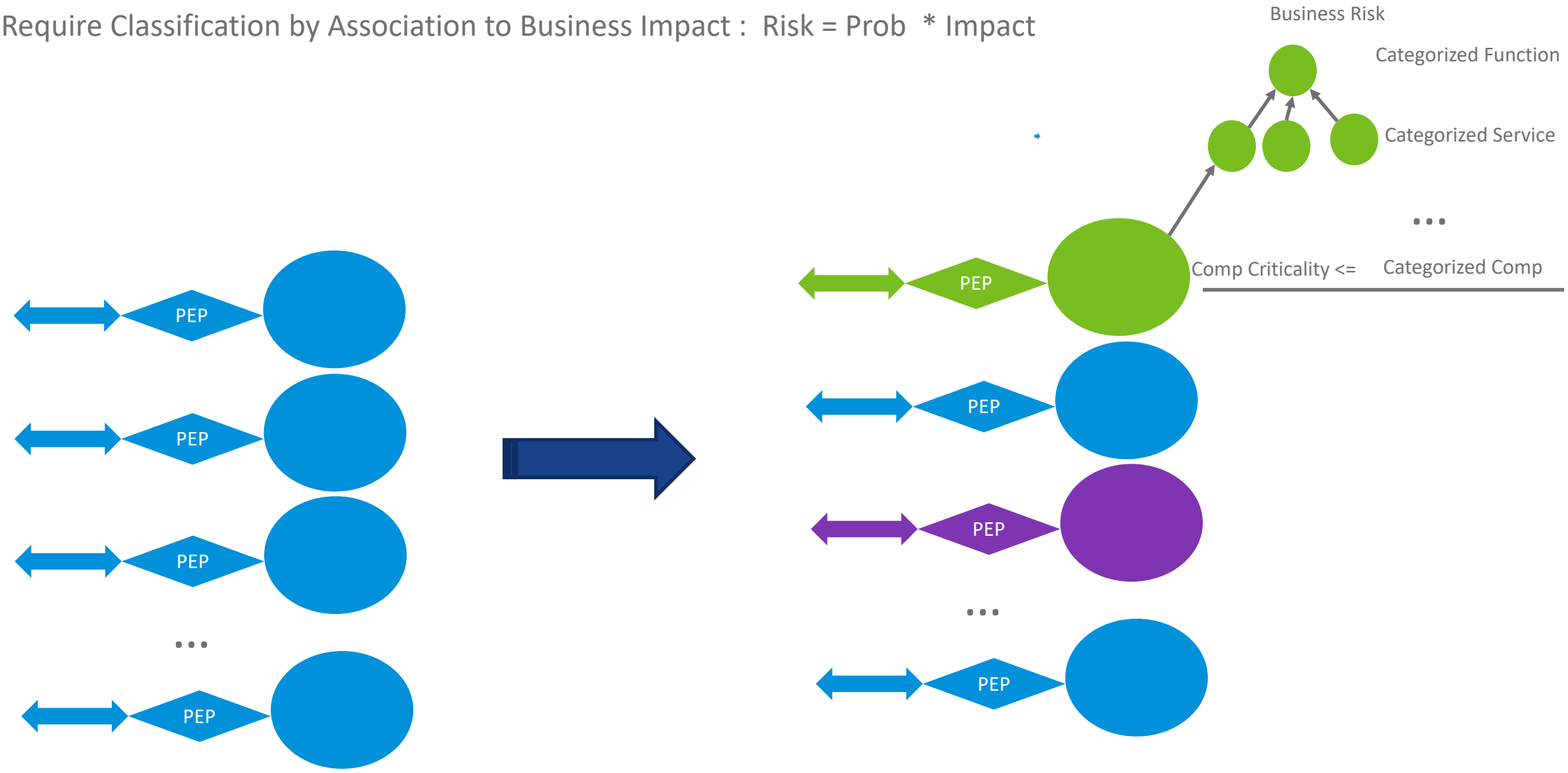
ZT Applies Compartment-specific policy, continuously.

Least Privilege +	Require knowing all “subjects”
Least Functionality +	Requires knowing all “objects”
Least Accessibility (crypt) +	Requires knowing access needs
Least Exposure (posture) +	Requires assessing device, service, platform integrity … dev due car, curation, testing
Coherence (peer, temporal)	Requires knowing intended, expected and observed behavior
…	

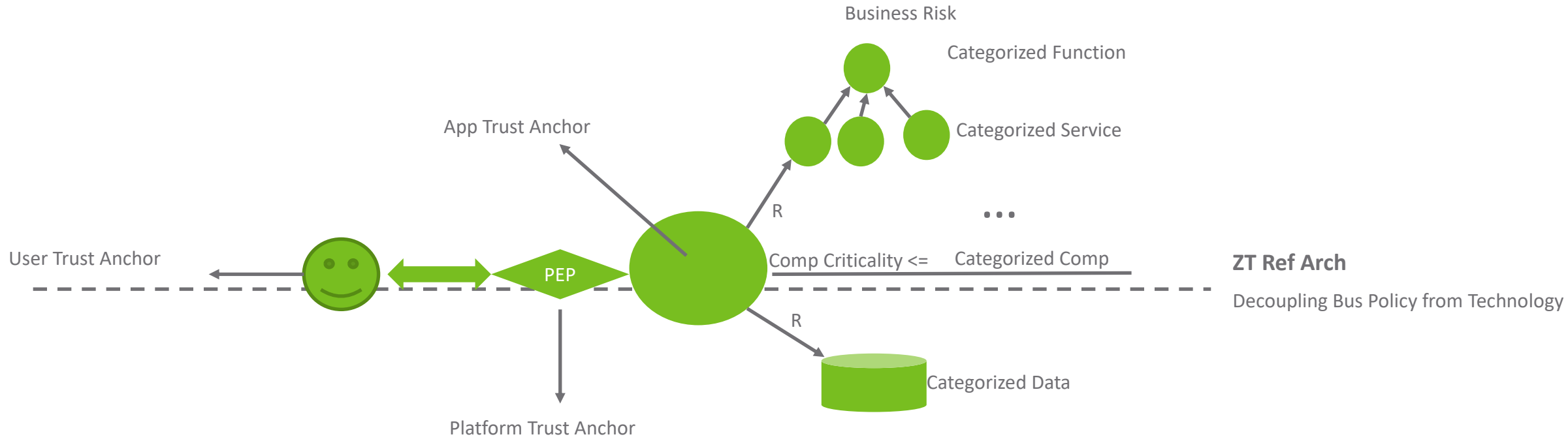


ZT Implies Many Continuous Enforcement Points … and Their Alerts

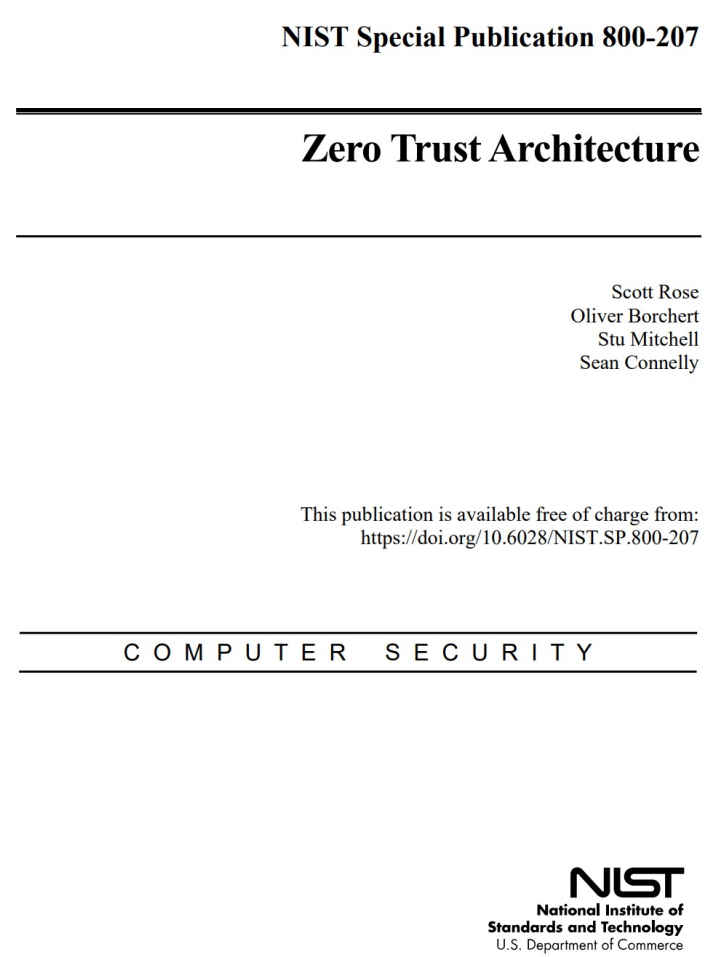
ZT Require Classification by Association to Business Impact : Risk = Prob * Impact



ZT Concept Space



ZT as of Q2 2021 – The Definitions that Matter



NIST Special Publication 800-207

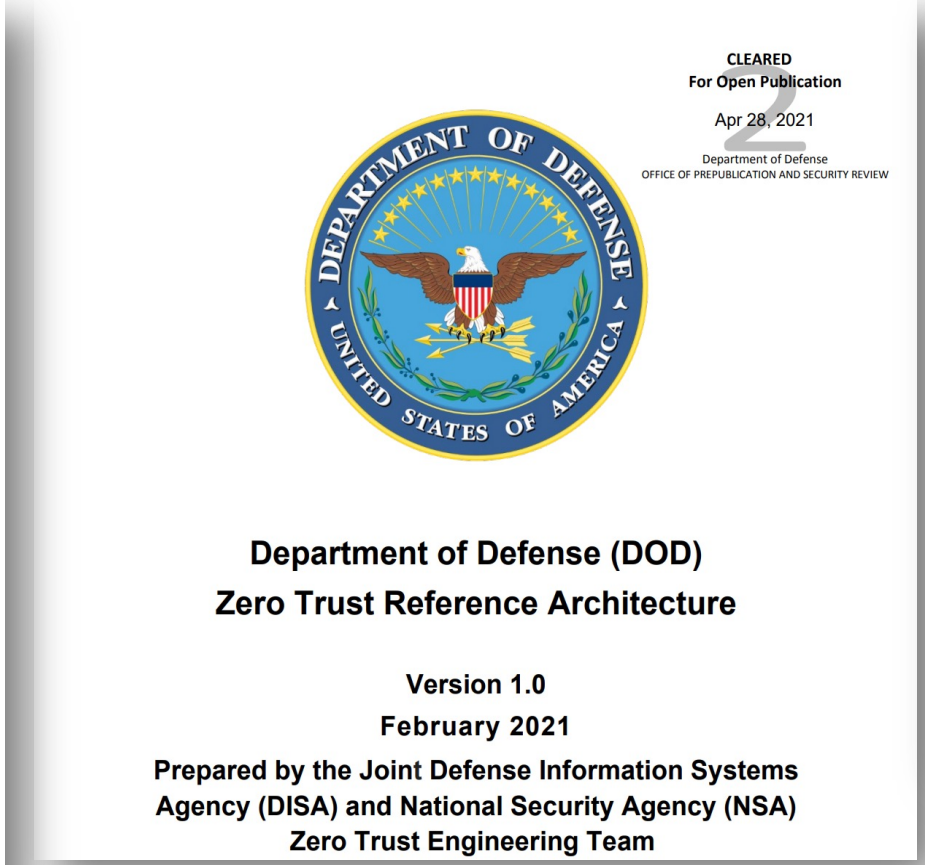
Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



CLEARED
For Open Publication
Apr 28, 2021
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DOD)
Zero Trust Reference Architecture

Version 1.0
February 2021

Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Systems that are designed using Zero Trust principals should be better positioned to address existing threats, but transitioning to such a system requires careful planning to avoid weakening the security posture along the way. NSA continues to monitor the technologies that can contribute to a Zero Trust solution and will provide additional guidance as warranted.

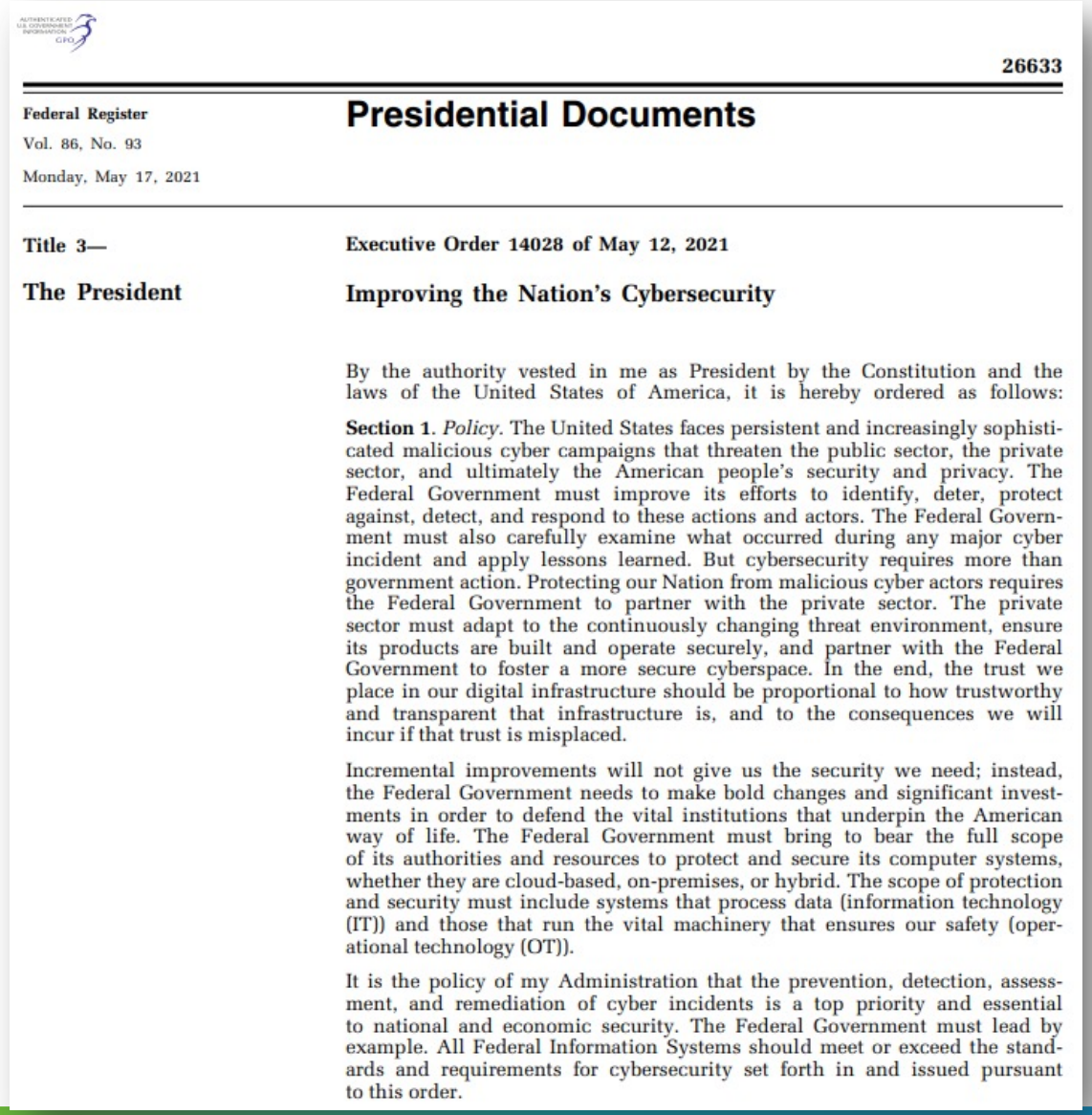
To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts must permeate most aspects of the network and its operations ecosystem. Organizations, from chief executive to engineer and operator, must understand and commit to the Zero Trust mindset before embarking on a Zero Trust path.

The following cybersecurity guidance explains the Zero Trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the Zero Trust model to achieve the desired results. The following recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

- *DISA and NSA, Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0*
- *NIST, SP 800-207, Zero Trust Architecture*
- *NSA, Embracing a Zero Trust Security Model*

Zero Trust – Why it matters? - The Mandate

https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity#:~:text=Executive%20Order%2014028%20of%20May%2012%2C%202021%20Improving,it%20is%20hereby%20ordered%20as%20follows%3A%20Section%201.



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

(k) the term "Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

What is Zero Trust?

High-Level ZT Implementation Architecture

What does ZTA look like … by definition.

ZT Architecture

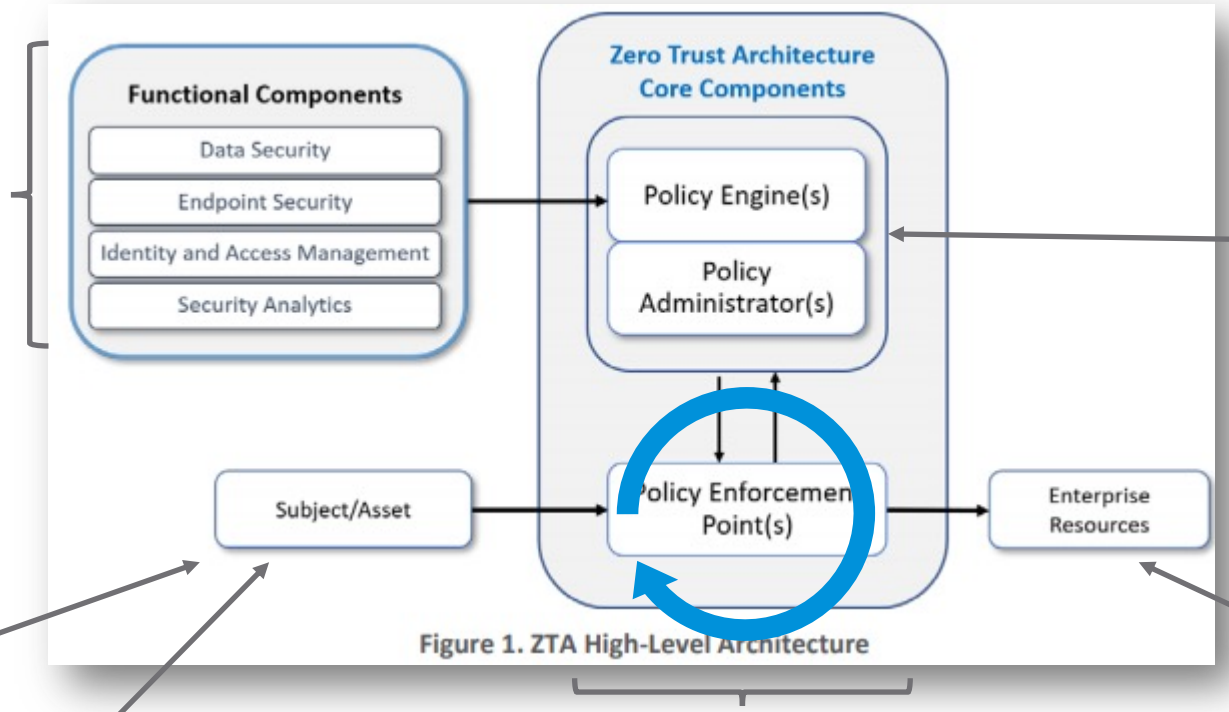


Figure 1. ZTA High-Level Architecture

Required ZT Solution Telemetry

- Aligned on same Subject, Object and associated Transactional (Business; Not CVSS Risk)

ZT Policy Statements

(e.g. OPA, …)

Subjects (Page 7)

- Users, Roles
- Service Accounts
- Identity Records (Rep)
- …

Assets (Page 8)

- Servers, Desktops (Page7)
- Laptops, Tablets, Phones
- Mobile & IoT Devices

Continuous Inline ZT Enforcement

- Logically Adjacent to Resources (Objects)
- Authoritative Controls and Independent Verification

Resources

- Applications
- Services
- Micro-services/Containers (NSA)
- (on Prem, Hosted, Cloud and Edge)

ZTA Implies Layering (end to end)

Enterprise Business aware ZT Policy

- Criticality Impact aware – real Risk
- Aligned from User To Enterprise Application
- Entitlement and Anomaly Informed

Risk Aware ZT Policy

e.g.: OPA + YAML + Stacklet

(Subject, Object, Criticality/Importance)

User/Device/App

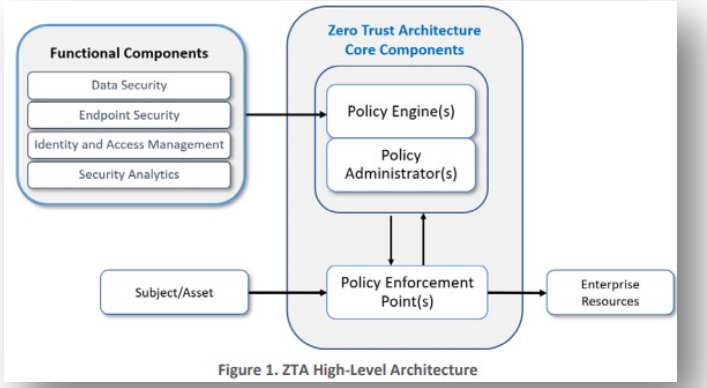


Figure 1. ZTA High-Level Architecture

Session/Host/Hosted Service

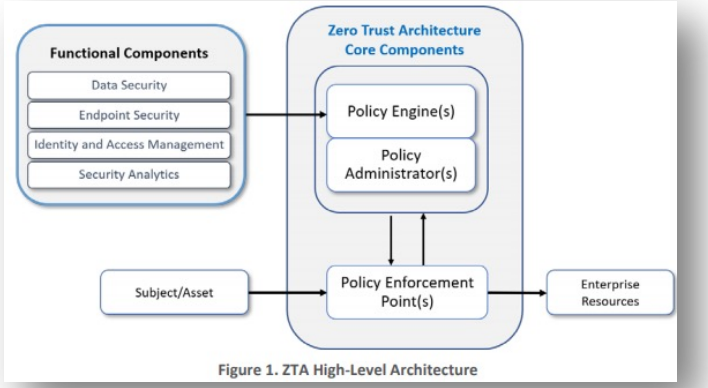


Figure 1. ZTA High-Level Architecture

ID/Container/Application-Micro-service, SM

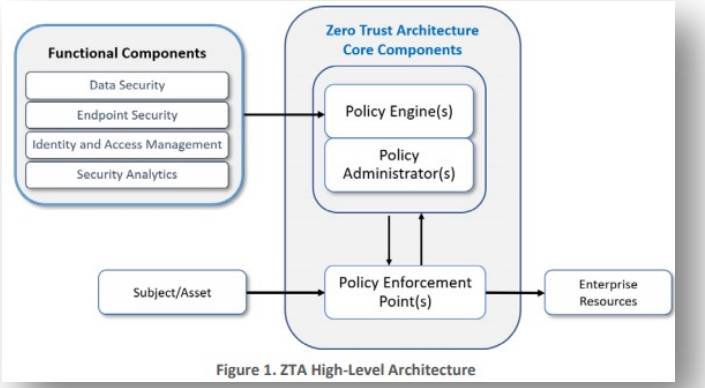


Figure 1. ZTA High-Level Architecture

Aligned ZT Conformant Policy (EU)
(Subject, Object, Criticality/Importance)

Aligned ZT Conformant Policy (GW)
(Subject, Object, Criticality/Importance)

Aligned ZT Conformant Policy (SM)
(Subject, Object, Criticality/Importance)

NSA Caveat on Partial ZTA Implementations (limited ZT protection)

When adding fractional ZT makes policy management less effective (NSA) Also see EO 10(k)

Enterprise Business aware ZT Policy

- Criticality Impact aware – real Risk
- Aligned from User To Enterprise Application
- Entitlement and Anomaly Informed

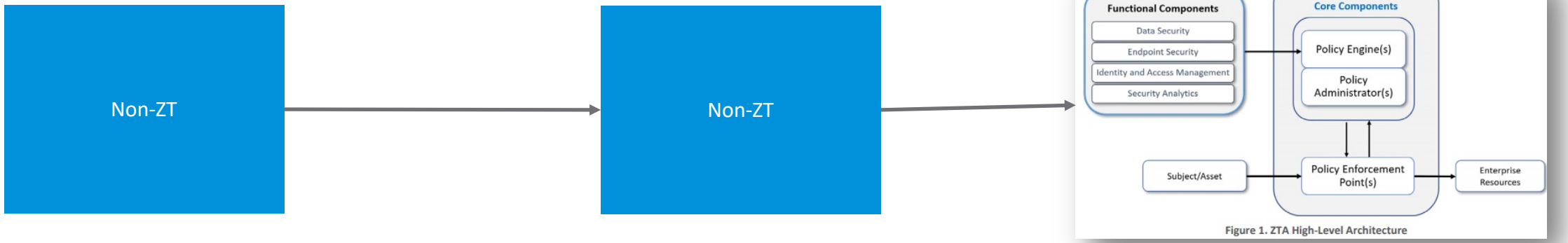
Conventional Policy Structure

(Non-ZT)

User/Device/App

Session/Host/Hosted Service

ID/Container/Application-Micro-service



Typically mis-aligned User/Device/App - Session/Host/Hosted Service

Mis-configured Intention (guard rails – Config, Roles, Classification) and Observation (verification – EDR, ML)

Traditional scattered security architecture (Policy aligned on VPN, VLAN, Perimeter, …)

False sense of ZT

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

CISA ZT Maturity Model (DRAFT - PC Opened 9/2021)

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

Zero Trust Maturity Model

Pre-decisional Draft

June 2021

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics	Automation and Orchestration	Governance		
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics	Automation and Orchestration	Governance		
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics	Automation and Orchestration	Governance		

Figure 2: High-Level Zero Trust Maturity Model

Important Observations from CISA ZT MM Document

[Page ii]

- The path to zero trust is an incremental process that will take years to implement.
- Legacy infrastructure and systems may not support a zero trust implementation.

[Page 2] Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time; for these reasons, moving to a ZTA is non-trivial. This provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. More fundamentally, zero trust may require a change in an organization's philosophy and culture around cybersecurity. The path to zero trust is a journey that will take years to implement.

[Page 3] 6. Challenge The Federal Government faces several challenges in transitioning to ZTA. First, legacy systems rely on "implicit trust"; this concept conflicts with the core principle of adaptive evaluation of trust within a ZTA. Additionally, existing infrastructures are also built on implicit trust and must either be rebuilt or replaced. To rebuild or replace information technology (IT) infrastructure and mission systems requires a significant investment on the part of agencies. Lastly, there is no consensus on or formal adoption of a maturity model for ZTA. While proposals for maturity models have been put forth, current initiatives for kickstarting zero trust adoption are often focused on the network layer and do not present a holistic approach for transition

CISA MM Transitioning to ZT [Page 4]

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

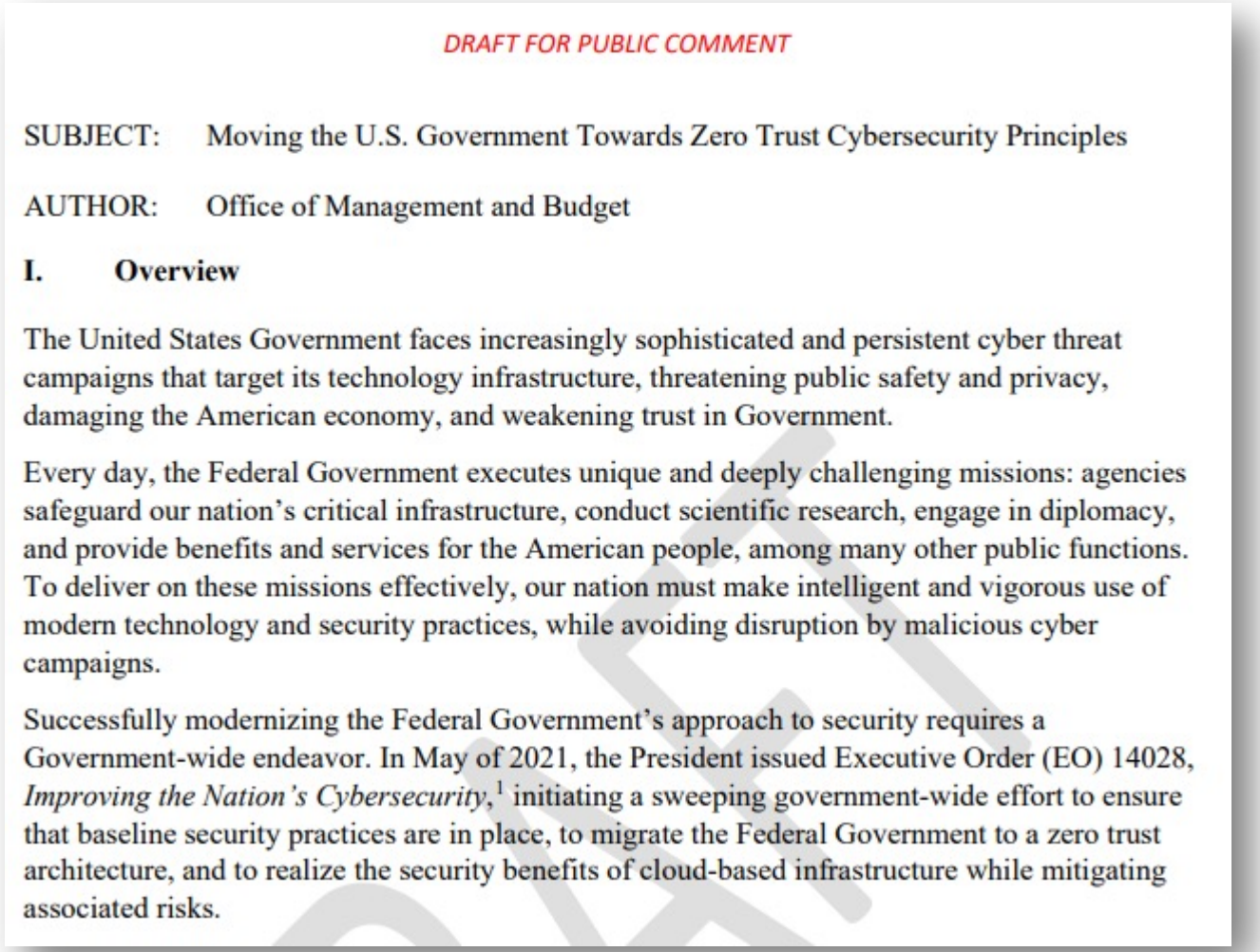
Transitioning to Zero Trust:

1. Identify Actors on the Enterprise.
2. Identify Assets Owned by the Enterprise.
3. Identify Key Processes and Evaluate Risks Associated with Executing Process.
   - The Basis for Business Impact (Risk)
4. Formulating Policies for the ZTA Candidate.
5. Identifying Candidate Solutions.
6. Initial Deployment and Monitoring

OMB Updates
M-Series Memos

OMB owns policy and contract language.

- Federal Zero Trust Strategy - Moving the U.S. Government Towards Zero Trust Cybersecurity Principles - https://zerotrust.cyber.gov/downloads/Office%20of%20Management%20and%20Budget%20-%20Federal%20Zero%20Trust%20Strategy%20-%20DRAFT%20For%20Public%20Comment%20-%202021-09-07.pdf



DRAFT FOR PUBLIC COMMENT

SUBJECT: Moving the U.S. Government Towards Zero Trust Cybersecurity Principles

AUTHOR: Office of Management and Budget

I. Overview

The United States Government faces increasingly sophisticated and persistent cyber threat campaigns that target its technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

Every day, the Federal Government executes unique and deeply challenging missions: agencies safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[1] initiating a sweeping government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

Where are we now?

What does ZT look over existing technology

DoD ZT Reference Architecture: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

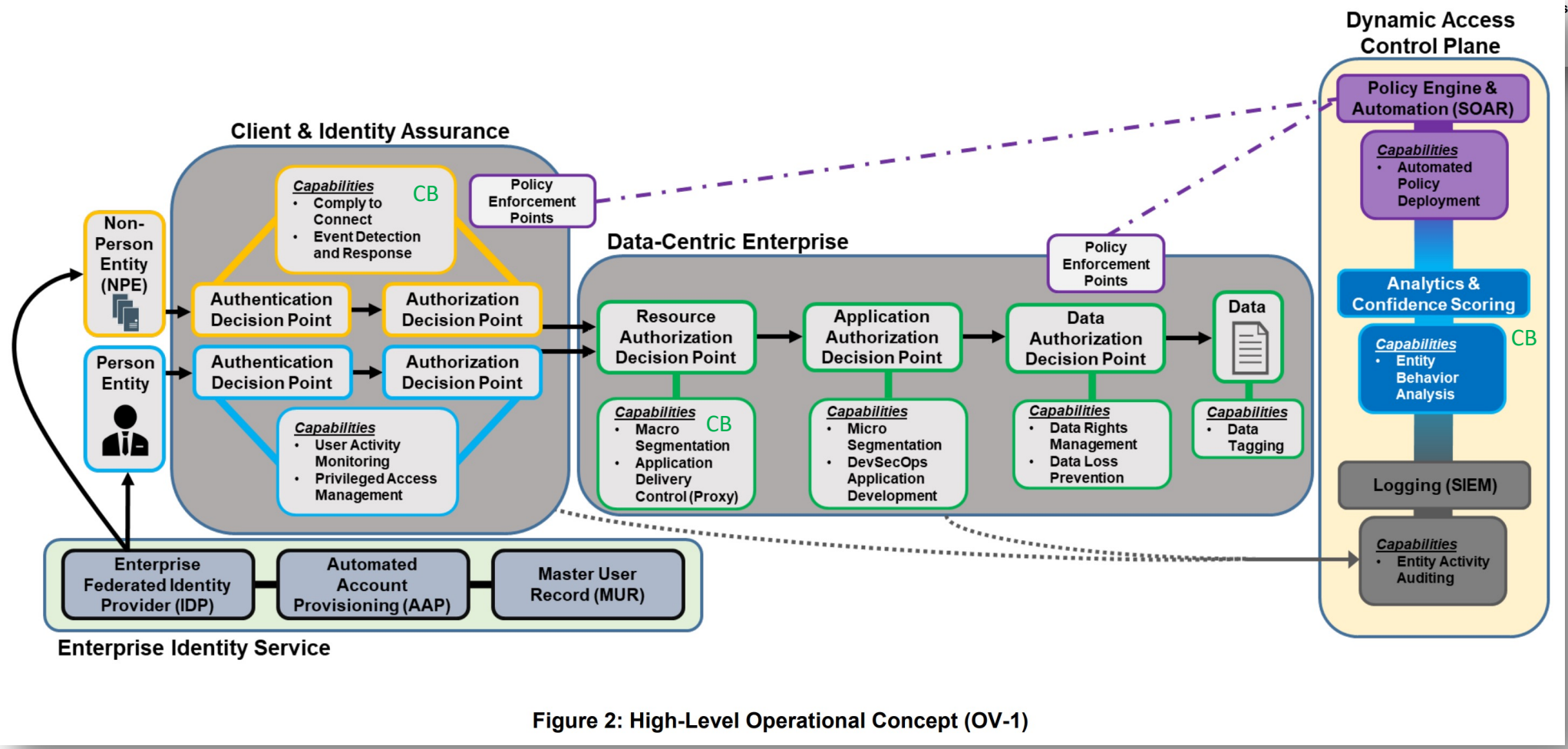


Figure 2: High-Level Operational Concept (OV-1)

CLEARED
For Open Publication
Apr 28, 2021
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Department of Defense (DOD)
t Reference Architecture

Version 1.0
February 2021

What does ZT look employing existing technology

DoD ZT Reference Architecture: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

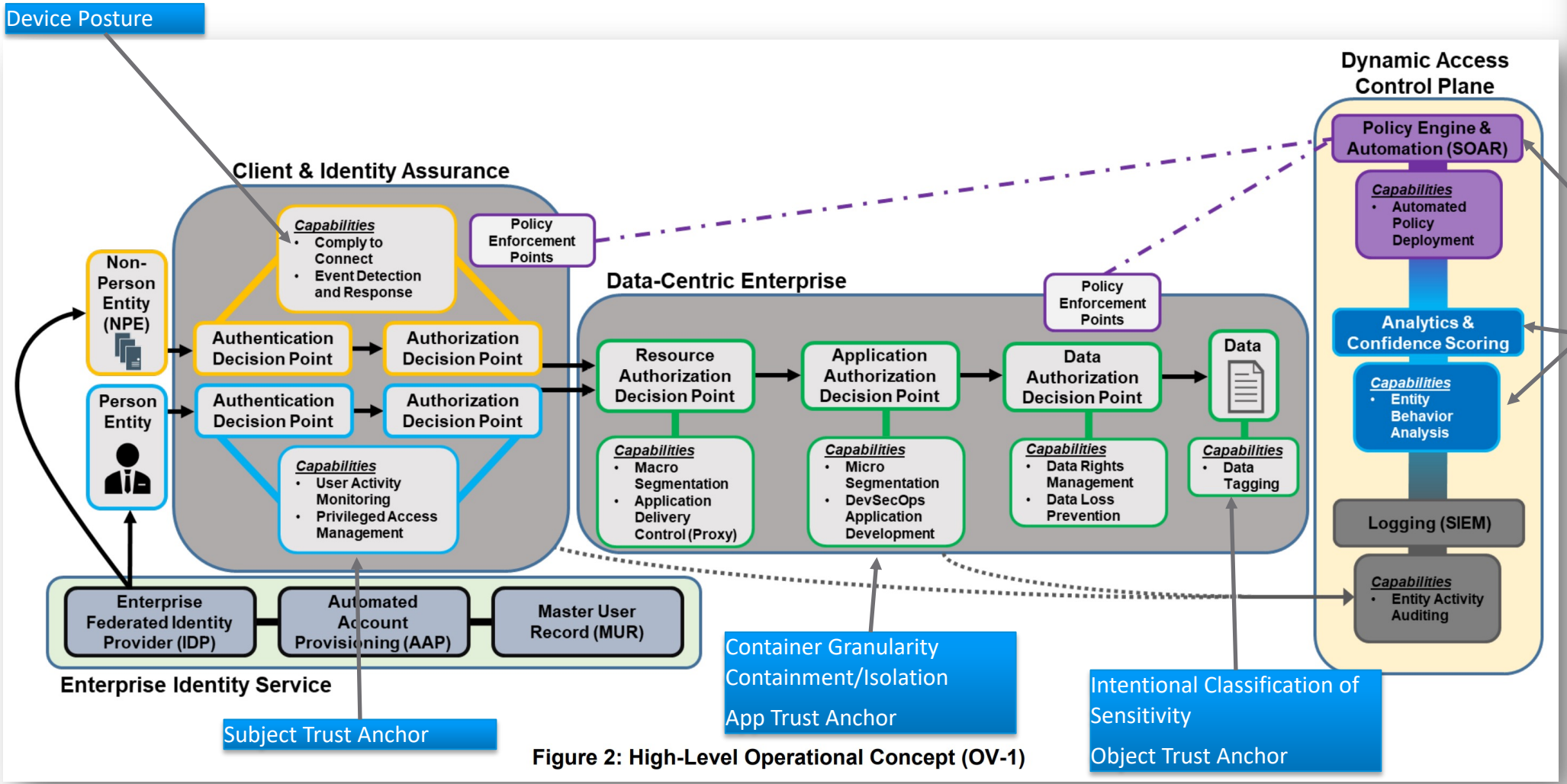
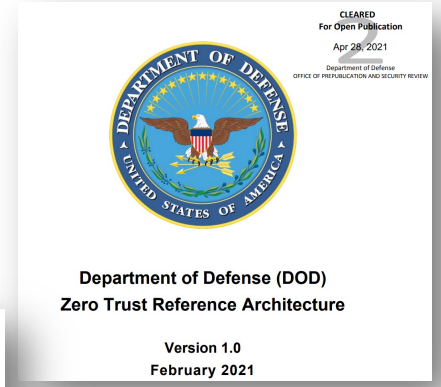


Figure 2: High-Level Operational Concept (OV-1)



ZT Policy Expression
- PEP Policy Deployment
- Subjects, Objects

Continuous Risk Eval

Application Trust Anchor based on "shifted left" security context

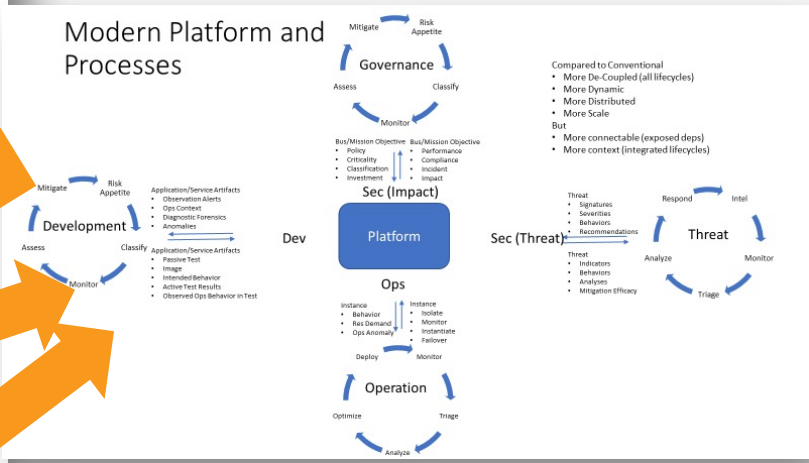
Guidelines on Minimum Standards for Developer Verification of Software

Paul E. Black
Barbara Guttman
Vadim Okun
Software and Systems Division
Information Technology Laboratory

July 2021

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Table of Contents



https://www.nist.gov/system/files/documents/2021/07/13/Developer%20Verification%20of%20Software.pdf

ZT Applies to Operation of “Critical Software”

… not just how you build secure stuff.

Security Measures for “EO-Critical Software” Use Under Executive Order (EO) 14028

July 9, 2021

Introduction

Executive Order (EO) 14028 on Improving the Nation’s Cybersecurity, May 12, 2021, directs the National Institute of Standards and Technology (NIST) to publish guidance on security measures for EO-critical software use, based on the definition of “EO-critical software” NIST developed for the EO.

> *(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.*

The EO directs the Office of Management and Budget (OMB) to require agencies to comply with the security measures guidance.

> *(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.*

To help identify and prioritize possible security measures for inclusion, NIST solicited position papers from the community, hosted a virtual workshop to gather input, consulted with the Cybersecurity & Infrastructure Security Agency (CISA) and OMB, and reviewed existing federal guidance on individual security measures that might apply to EO-critical software use.

This document starts with information about the purpose and scope of the guidance, including the meaning of “EO-critical software use.” Next, it defines the fundamental security measures for EO-critical software use. It concludes with Frequently Asked Questions (FAQ) that provide additional information on the guidance and its relationship to other tasks in the EO and to other federal cybersecurity initiatives. The last item in the FAQ is a summary of the security measures.

SM 1.4: Employ boundary protection techniques as appropriate to minimize direct access to EO-critical software, EO-critical software platforms, and associated data. Examples of such techniques include network segmentation, isolation, software-defined perimeters, and proxies.	▪ **NIST,** Cybersecurity Framework**:** PR.AC-3, PR.AC-5 ▪ **NIST,** SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations: SC-7 ▪ **CISA**, Continuous Diagnostics and Mitigation Program: Network Security Management – What is Happening on the Network? How is the Network Protected? ▪ **CISA,** Defending Against Software Supply Chain Attacks ▪ **CISA**, Securing Network Infrastructure Devices ▪ **CISA**, Trusted Internet Connections 3.0: Traditional TIC Use Case ▪ **NIST,** SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy ▪ **NIST,** SP 800-207, Zero Trust Architecture ▪ **NSA,** Segment Networks and Deploy Application-Aware Defenses

Zero Trust cited in 10 separate audit controls for the compliant and certifiable operation of “Critical Software”. ZT is not just a product capability for customers, it is also the kind of policy that is expected to constrain thecutomer’s operation of our platform.

https://www.nist.gov/system/files/documents/2021/07/09/Critical%20Software%20Use%20Security%20Measures%20Guidance.pdf

Enter NIST NCCoE

https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE | NIST National Institute of Standards and Technology U.S. Department of Commerce

Search ...

Sign up for newsletter

About the Center | Projects | Partners | News | Events | Library

NCCoE Announces Technology Collaborators to Demonstrate Zero Trust Architectures

Wednesday, July 21, 2021 | NIST NCCoE

The National Cybersecurity Center of Excellence (NCCoE) will be joined by the following technology collaborators in their Implementing a Zero Trust Architecture Project:

- Amazon Web Services, Inc.
- Appgate
- Cisco Systems, Inc.
- F5 Networks, Inc.
- FireEye, Inc.
- Forescout Technologies, Inc.
- International Business Machines Corporation (IBM)
- McAfee Corp.
- Microsoft Corporation
- MobileIron, Inc. an Ivanti Company
- Okta, Inc.
- Palo Alto Networks
- PC Matic, Inc.
- Radiant Logic, Inc.
- SailPoint Technologies, Inc.
- Symantec, a Division of Broadcom
- Tenable, Inc.
- Zscaler, Inc.

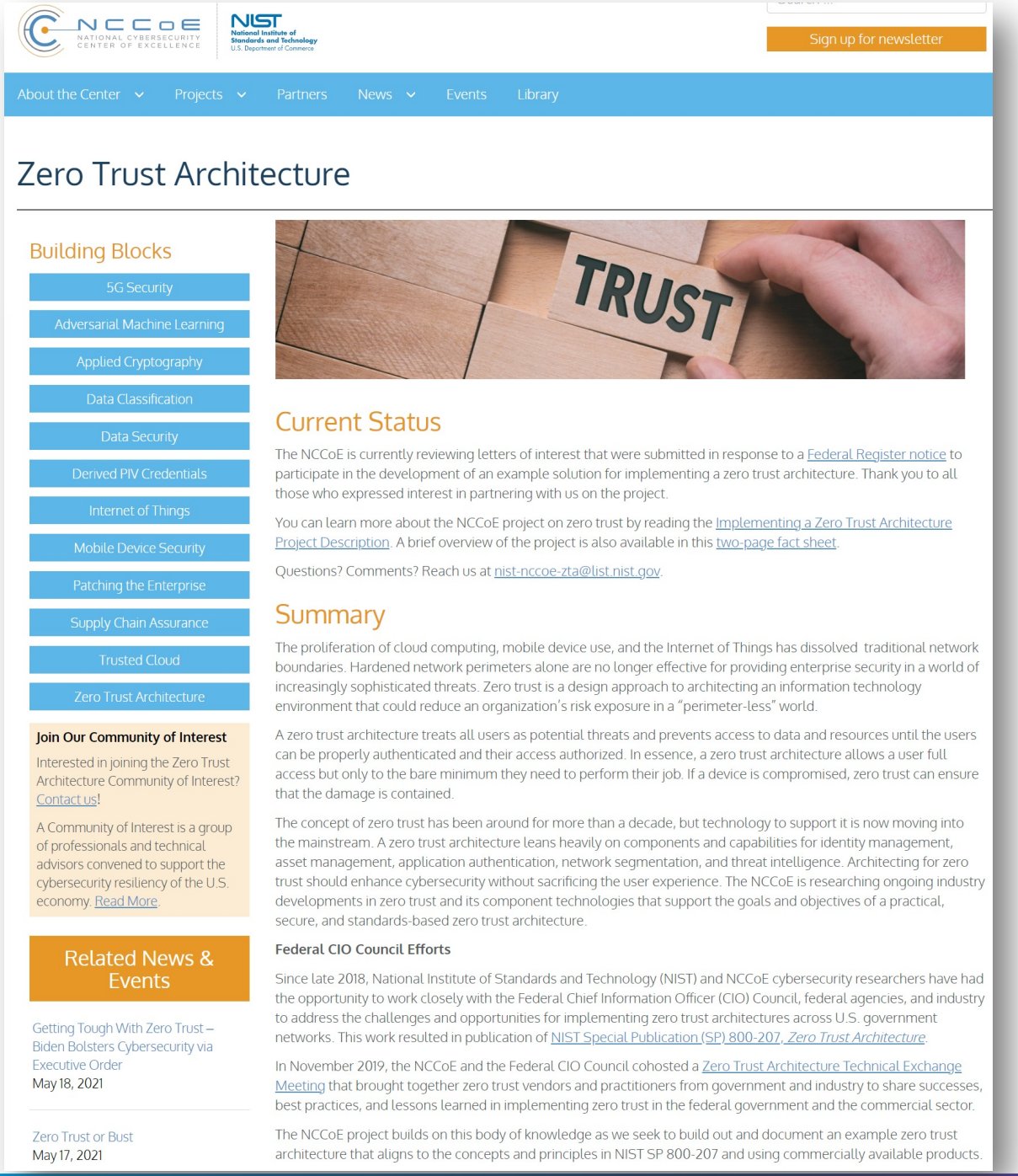
These collaborators will work with the NCCoE to demonstrate several approaches to implementing zero trust architectures, which will be designed and deployed according to the concepts and tenets documented in NIST SP 800-207, *Zero Trust Architecture*.

"We received an overwhelming response from the vendor community on this important project," said Natalia Martin, acting director of the NCCoE. "Implementing a zero trust architecture has become a federal cybersecurity mandate and a business imperative. We are excited to work with industry demonstrating various approaches to implementing a zero trust architecture using a diverse mix of vendor products and capabilities, and share how-to guidance and lessons learned from the experience."

Each of these organizations responded to a notice in the Federal Register to submit capabilities that aligned with desired solution characteristics for the project. The accepted collaborators were extended a Cooperative Research and Development Agreement, enabling them to take part in a consortium in which they will contribute expertise and hardware or software to help refine a reference design and build example standards-based solutions.

The NCCoE project will result in a publicly available NIST Cybersecurity Practice Guide in the Special Publication 1800 series, a detailed guide describing the practical steps needed to implement the cybersecurity reference designs.

To learn more about this project, visit the Zero Trust Architecture project page. To receive news and information about our progress, please join the Zero Trust Architecture Community of Interest.



NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE | NIST National Institute of Standards and Technology U.S. Department of Commerce

Sign up for newsletter

About the Center | Projects | Partners | News | Events | Library

Zero Trust Architecture

Building Blocks

- 5G Security
- Adversarial Machine Learning
- Applied Cryptography
- Data Classification
- Data Security
- Derived PIV Credentials
- Internet of Things
- Mobile Device Security
- Patching the Enterprise
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

Join Our Community of Interest

Interested in joining the Zero Trust Architecture Community of Interest? Contact us!

A Community of Interest is a group of professionals and technical advisors convened to support the cybersecurity resiliency of the U.S. economy. Read More.

Related News & Events

Getting Tough With Zero Trust – Biden Bolsters Cybersecurity via Executive Order
May 18, 2021

Zero Trust or Bust
May 17, 2021

Current Status

The NCCoE is currently reviewing letters of interest that were submitted in response to a Federal Register notice to participate in the development of an example solution for implementing a zero trust architecture. Thank you to all those who expressed interest in partnering with us on the project.

You can learn more about the NCCoE project on zero trust by reading the Implementing a Zero Trust Architecture Project Description. A brief overview of the project is also available in this two-page fact sheet.

Questions? Comments? Reach us at nist-nccoe-zta@list.nist.gov.

Summary

The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of increasingly sophisticated threats. Zero trust is a design approach to architecting an information technology environment that could reduce an organization's risk exposure in a "perimeter-less" world.

A zero trust architecture treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized. In essence, a zero trust architecture allows a user full access but only to the bare minimum they need to perform their job. If a device is compromised, zero trust can ensure that the damage is contained.

The concept of zero trust has been around for more than a decade, but technology to support it is now moving into the mainstream. A zero trust architecture leans heavily on components and capabilities for identity management, asset management, application authentication, network segmentation, and threat intelligence. Architecting for zero trust should enhance cybersecurity without sacrificing the user experience. The NCCoE is researching ongoing industry developments in zero trust and its component technologies that support the goals and objectives of a practical, secure, and standards-based zero trust architecture.

Federal CIO Council Efforts

Since late 2018, National Institute of Standards and Technology (NIST) and NCCoE cybersecurity researchers have had the opportunity to work closely with the Federal Chief Information Officer (CIO) Council, federal agencies, and industry to address the challenges and opportunities for implementing zero trust architectures across U.S. government networks. This work resulted in publication of NIST Special Publication (SP) 800-207, *Zero Trust Architecture*.

In November 2019, the NCCoE and the Federal CIO Council cohosted a Zero Trust Architecture Technical Exchange Meeting that brought together zero trust vendors and practitioners from government and industry to share successes, best practices, and lessons learned in implementing zero trust in the federal government and the commercial sector.

The NCCoE project builds on this body of knowledge as we seek to build out and document an example zero trust architecture that aligns to the concepts and principles in NIST SP 800-207 and using commercially available products.

NCCoE Names 18 Firms for Zero Trust Collaboration Project | NCCoE (nist.gov)

NCCoE Names 18 Firms for Zero Trust Collaboration Project
Friday, July 23, 2021

The National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) has named 18 firms it will work with on NCCoE's Implementing a Zero Trust Architecture Project.
The 18 companies – all of whom answered a public call for collaborators and entered a related cooperative research and development agreement with NCCoE – will work with the organization to demonstrate approaches to implementing zero trust architectures designed and deployed according the concepts and tenets in NIST's Special Publication (SP) 800-207 on Zero Trust Architecture.

The goal of the project is to produce a publicly available NIST Cybersecurity Practice Guide that shows the practical steps to implement the cybersecurity reference designs. Natalia Martin, NCCoE's acting director, said the center received "an overwhelming response from the vendor community on this important project."

"Implementing a zero trust architecture has become a Federal cybersecurity mandate and a business imperative," she said. "We are excited to work with industry demonstrating various approaches to implementing a zero trust architecture using a diverse mix of vendor products and capabilities, and share how-to guidance and lessons learned from the experience."

The 18 firms are: Amazon Web Services, Inc.; Appgate; Cisco Systems, Inc.; F5 Networks, Inc.; FireEye, Inc.; Forescout Technologies, Inc.; International Business Machines Corporation (IBM); McAfee Corp.; Microsoft Corporation; MobileIron, Inc. an Ivanti Company; Okta, Inc.; Palo Alto Networks; PC Matic, Inc.; Radiant Logic, Inc.; SailPoint Technologies, Inc.; Symantec, a Division of Broadcom; Tenable, Inc.; and Zscaler, Inc.

"Zero trust is a team sport and the NIST NCCoE is taking the initiative to bring together best-of-breed zero trust leaders," commented Stephen Kovac, Vice President of Global Government and Head of Corporate Compliance at Zscaler.

"We are all committed to collaborating and demonstrating different, practical approaches to implement a zero trust architecture," he said. "As we know, no one solution fits every situation. Zscaler is honored to be a part of this coalition working side by side to realize the opportunity for zero trust to strengthen every agency's cyber defenses."
"Cisco is happy to be a National Center of Excellence Partner (NCEP) of NCCoE since the beginning and are proud to continue contributing to their SP 1800 documents," said Peter Romness, Cybersecurity Principal, U.S. Public Sector CTO Office, at Cisco. "These publications are used by governments and businesses around the world has guides to implement their own cybersecurity capabilities."
"Zero Trust is a hot topic and our customers are looking for guidance from an impartial, trusted source like NIST," he said. "Their SP 800-207 – Zero Trust Architecture, is already being used to understand zero trust. This new project will show examples of how to implement zero trust. We're thrilled we were selected to help."

NCCoE Evaluation Comparative Scenarios (Pages 5-6)

May be phased due to market balkanization of policy across segments and telemetries.

Scenario 1: Employee Access to Corporate Resources An employee is looking for easy and secure access to corporate resources, from any work location.

Scenario 2: Employee Access to Internet Resources An employee is trying to access the public internet to accomplish some tasks.

Scenario 3: Contractor Access to Corporate and Internet Resources A contractor is trying to access certain corporate resources and the internet.

Scenario 4: Inter-server Communication Within the Enterprise Corporate services often have different servers communicating with each other. For example, a web server communicates with an application server.

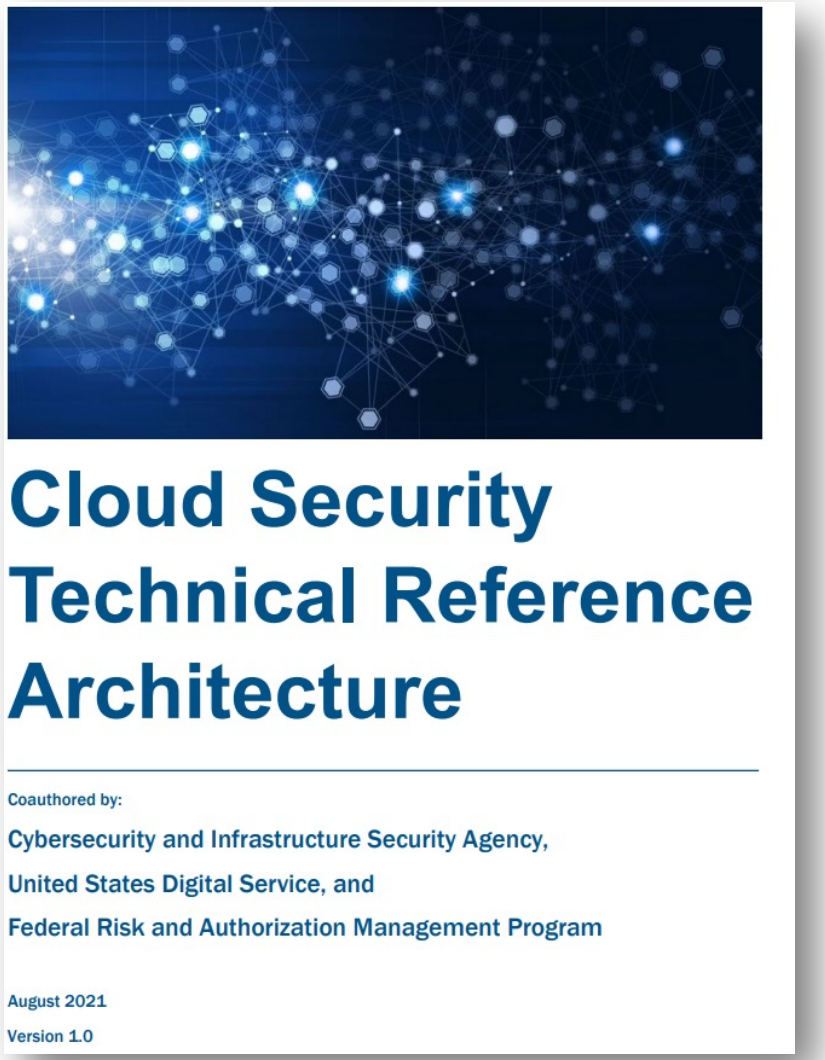
Scenario 5: Cross-Enterprise Collaboration with Business Partners Two enterprises In this scenario, the ZTA solution implemented in this project will enable users from one enterprise to securely access specific resources from the other enterprise, and vice versa.

Scenario 6: Develop Trust Score/Confidence Level with Corporate Resources. . In this scenario, a ZTA solution will integrate these monitoring and SIEM systems with the policy engine to produce more precise calculation of trust scores/confidence levels in near real time.

https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf

CISA Cloud Security Ref Arch (DRAFT - PC Opened 9/2021)

https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf



CISA CSRA Refers to Zero Trust 38 times:

"…

As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt zero trust architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with zero trust architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the FedRAMP within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

[…]

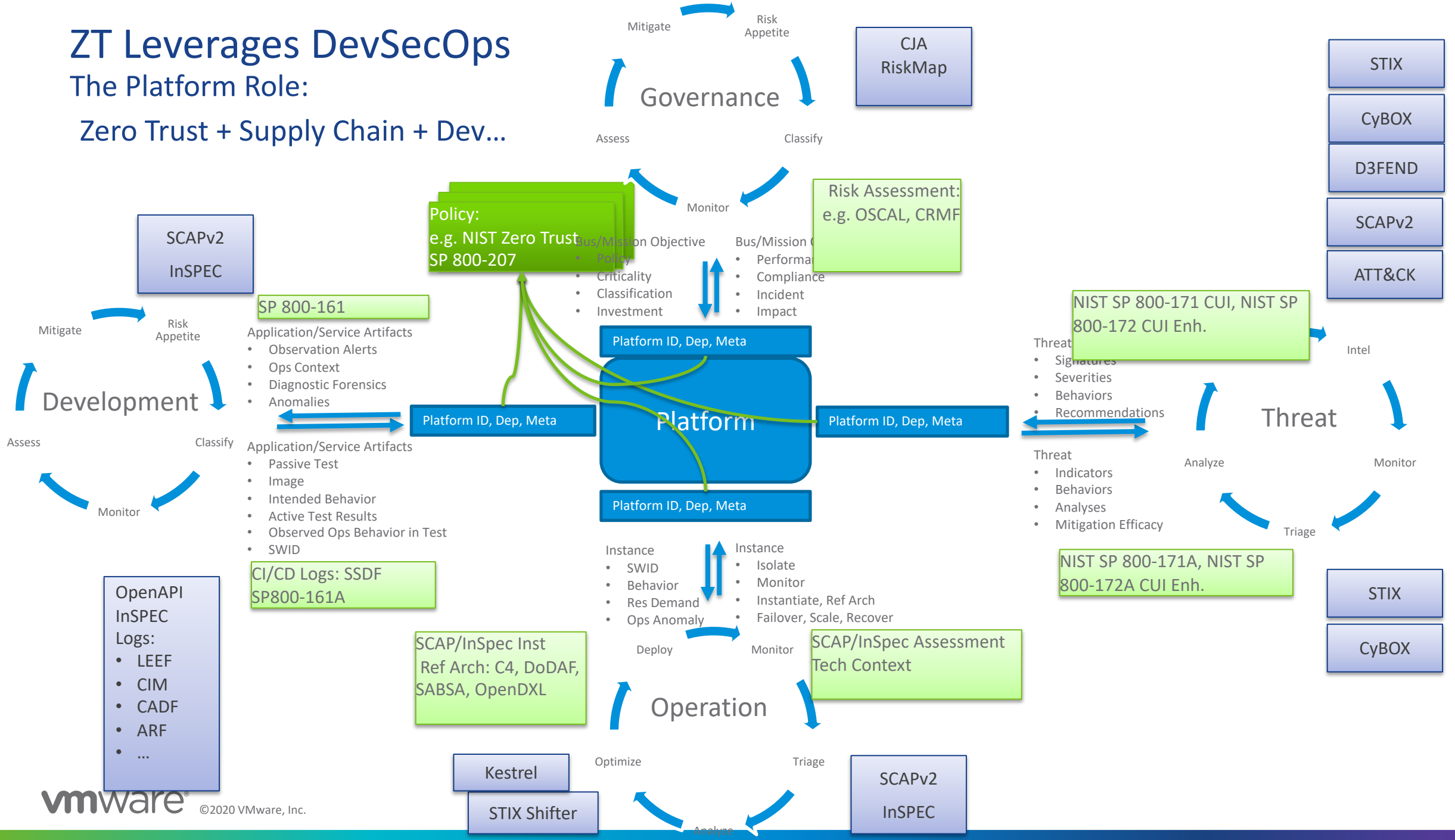
Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the Federal Civilian Executive Branch (FCEB), cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

…"

ZT Leverages DevSecOps

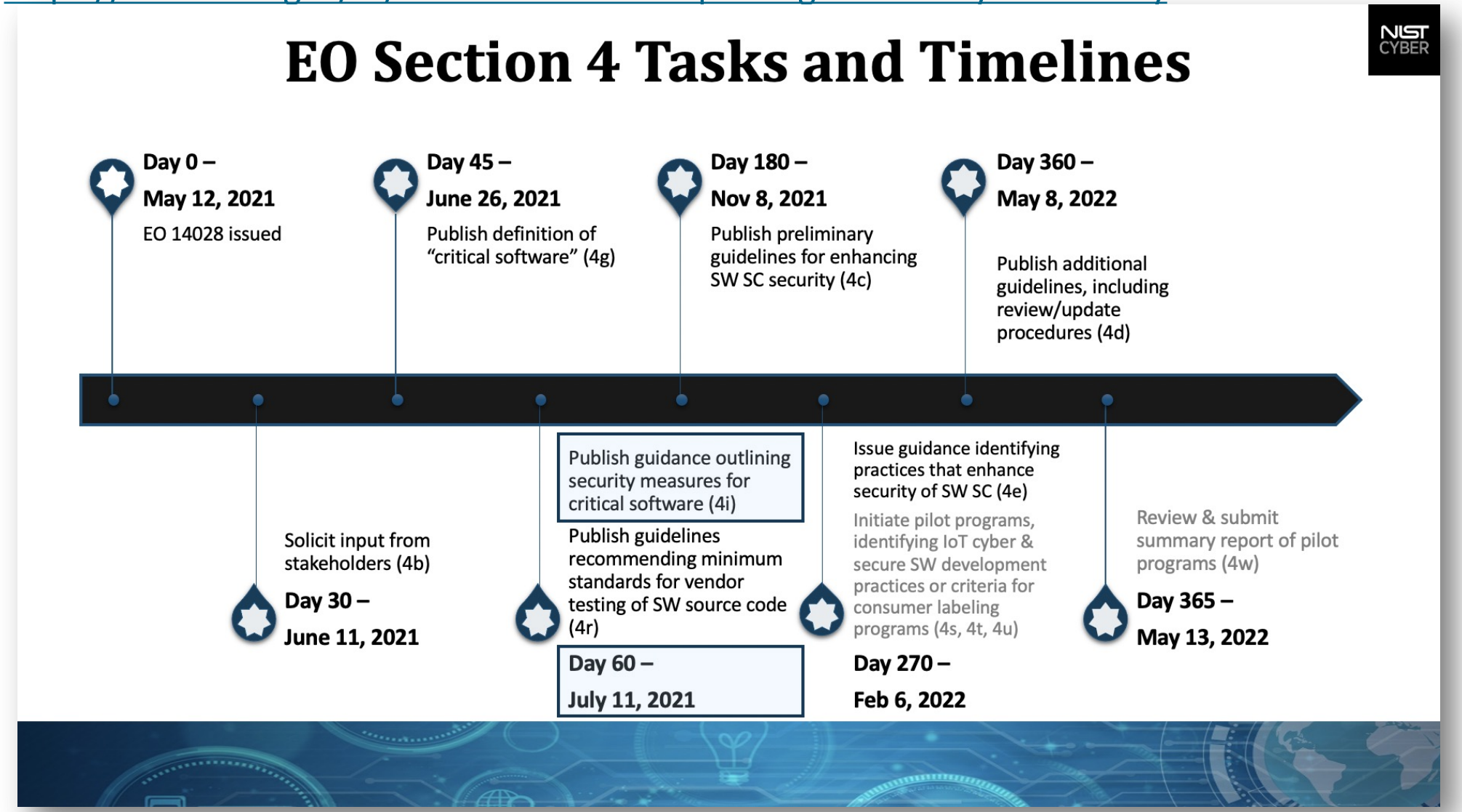
The Platform Role:

Zero Trust + Supply Chain + Dev…



NIST and the EO 14028 (Where ZT is headed)

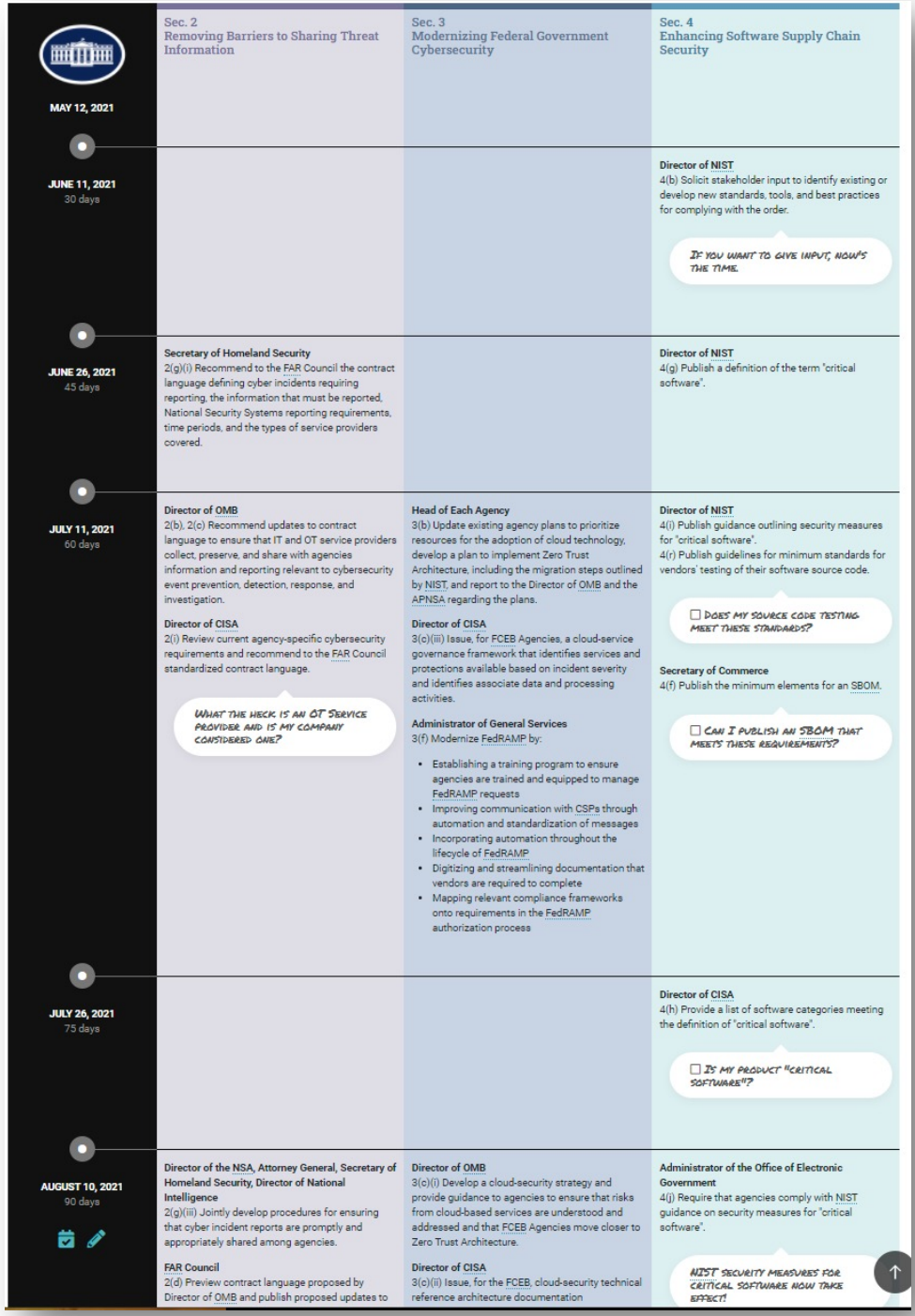
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity



Scope + Timeline

EO-14028 Timeline (Adolus)

- https://info.adolus.com/eo14028-timeline
- Demostrates progressive refinement of requirements as they eminate from NIST, CISA, OMB, and FAR changes.



	Sec. 2 Removing Barriers to Sharing Threat Information	Sec. 3 Modernizing Federal Government Cybersecurity	Sec. 4 Enhancing Software Supply Chain Security
MAY 12, 2021			
JUNE 11, 2021 30 days			**Director of NIST** 4(b) Solicit stakeholder input to identify existing or develop new standards, tools, and best practices for complying with the order. *If you want to give input, now's the time.*
JUNE 26, 2021 45 days	**Secretary of Homeland Security** 2(g)(i) Recommend to the FAR Council the contract language defining cyber incidents requiring reporting, the information that must be reported, National Security Systems reporting requirements, time periods, and the types of service providers covered.		**Director of NIST** 4(g) Publish a definition of the term "critical software".
JULY 11, 2021 60 days	**Director of OMB** 2(b), 2(c) Recommend updates to contract language to ensure that IT and OT service providers collect, preserve, and share with agencies information and reporting relevant to cybersecurity event prevention, detection, response, and investigation. **Director of CISA** 2(i) Review current agency-specific cybersecurity requirements and recommend to the FAR Council standardized contract language. *What the heck is an OT Service Provider and is my company considered one?*	**Head of Each Agency** 3(b) Update existing agency plans to prioritize resources for the adoption of cloud technology, develop a plan to implement Zero Trust Architecture, including the migration steps outlined by NIST, and report to the Director of OMB and the APNSA regarding the plans. **Director of CISA** 3(c)(iii) Issue, for FCEB Agencies, a cloud-service governance framework that identifies services and protections available based on incident severity and identifies associate data and processing activities. **Administrator of General Services** 3(f) Modernize FedRAMP by: • Establishing a training program to ensure agencies are trained and equipped to manage FedRAMP requests • Improving communication with CSPs through automation and standardization of messages • Incorporating automation throughout the lifecycle of FedRAMP • Digitizing and streamlining documentation that vendors are required to complete • Mapping relevant compliance frameworks onto requirements in the FedRAMP authorization process	**Director of NIST** 4(i) Publish guidance outlining security measures for "critical software". 4(r) Publish guidelines for minimum standards for vendors' testing of their software source code. ☐ *Does my source code testing meet these standards?* **Secretary of Commerce** 4(f) Publish the minimum elements for an SBOM. ☐ *Can I publish an SBOM that meets these requirements?*
JULY 26, 2021 75 days			**Director of CISA** 4(h) Provide a list of software categories meeting the definition of "critical software". ☐ *Is my product "critical software"?*
AUGUST 10, 2021 90 days	**Director of the NSA, Attorney General, Secretary of Homeland Security, Director of National Intelligence** 2(g)(iii) Jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies. **FAR Council** 2(d) Preview contract language proposed by Director of OMB and publish proposed updates to	**Director of OMB** 3(c)(i) Develop a cloud-security strategy and provide guidance to agencies to ensure that risks from cloud-based services are understood and addressed and that FCEB Agencies move closer to Zero Trust Architecture. **Director of CISA** 3(c)(ii) Issue, for the FCEB, cloud-security technical reference architecture documentation	**Administrator of the Office of Electronic Government** 4(j) Require that agencies comply with NIST guidance on security measures for "critical software". *NIST security measures for critical software now take effect!*

Zero Trust - UK

NSCS Zero Trust Architecture –
https://www.ncsc.gov.uk/collection/zero-trust-architecture
https://www.ncsc.gov.uk/section/ncsc-for-startups/overview
https://www.ncsc.gov.uk/blog-post/zero-trust-1-0

UK NCSC ZT Architecture Principles

1. Know your architecture, including users, devices, services and data.
2. Know your User, Service and Device identities.
3. Assess your user behaviour, device and service health.
4. Use policies to authorise requests.
5. Authenticate & Authorise everywhere.
6. Focus your monitoring on users, devices and services.
7. Don't trust any network, including your own.
8. Choose services designed for zero trust.

EU NIS2 and ZT – Parliament Vote now in November

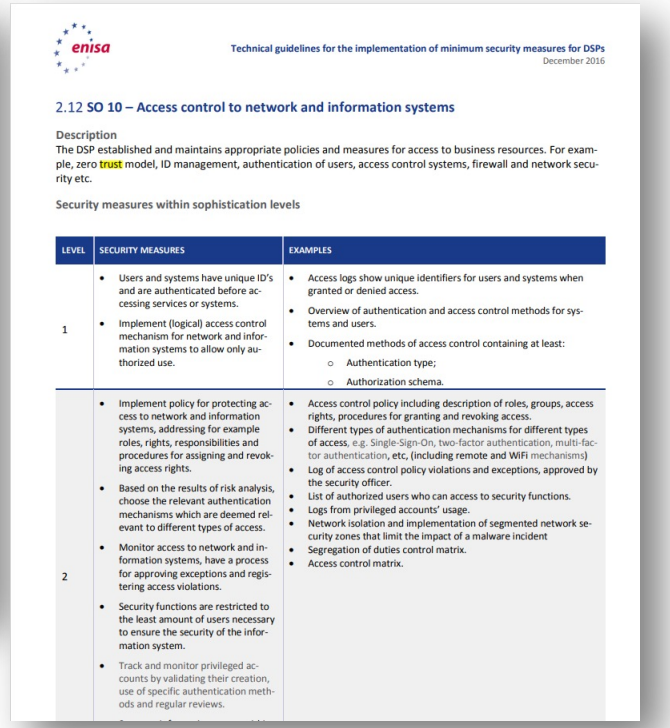
06_ Reduction of false positives. This long waited promise is key in the future of the cybersecurity industry and in the fight against the alarm fatigue.

07_ Zero-trust security strategies. With an increasing pressure on IT systems from new business requirements such as remote working, digitalization of the business model and data sprawl, zero trust is seen by many decision makers as the solution de facto to secure corporate assets.

08_ Enterprise cloud migration errors. With many businesses migrating their data to cloud-based solutions, the number of configuration errors will increase exposing data to a potential breach. Cloud service providers will address the issue by implementing systems that identify these type of errors automatically.

09_ Hybrid threats. New *modus operandi* adopt virtual and physical world threats. The spread of disinformation or fake news for example, is a key fixture of the hybrid threat landscape. The EUvsDisinfo[11] is a flagship project of the European External Action Service's East StratCom Task Force established to address the disinformation threat.

10_ The attractiveness of the cloud infrastructure as a target will grow. The increasing reliance on public cloud infrastructure will surge the risk of outages. Misconfiguration of cloud resources is still the number one cause for cloud attacks, but attacks aiming directly at the cloud services providers gaining popularity among hackers.



enisa

Technical guidelines for the implementation of minimum security measures for DSPs
December 2016

2.12 **SO 10 – Access control to network and information systems**

Description
The DSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES

1	• Users and systems have unique ID's and are authenticated before accessing services or systems.
	• Implement (logical) access control mechanism for network and information systems to allow only authorized use.
		• Access logs show unique identifiers for users and systems when granted or denied access.
		• Overview of authentication and access control methods for systems and users.
		• Documented methods of access control containing at least:
		  ○ Authentication type;
		  ○ Authorization schema.

2	• Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. • Based on the results of risk analysis, choose the relevant authentication mechanisms which are deemed relevant to different types of access. • Monitor access to network and information systems, have a process for approving exceptions and registering access violations. • Security functions are restricted to the least amount of users necessary to ensure the security of the information system. • Track and monitor privileged accounts by validating their creation, use of specific authentication methods and regular reviews.	• Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. • Different types of authentication mechanisms for different types of access, e.g. Single-Sign-On, two-factor authentication, multi-factor authentication, etc, (including remote and WiFi mechanisms) • Log of access control policy violations and exceptions, approved by the security officer. • List of authorized users who can access to security functions. • Logs from privileged accounts' usage. • Network isolation and implementation of segmented network security zones that limit the impact of a malware incident • Segregation of duties control matrix. • Access control matrix.

Look Familiar??

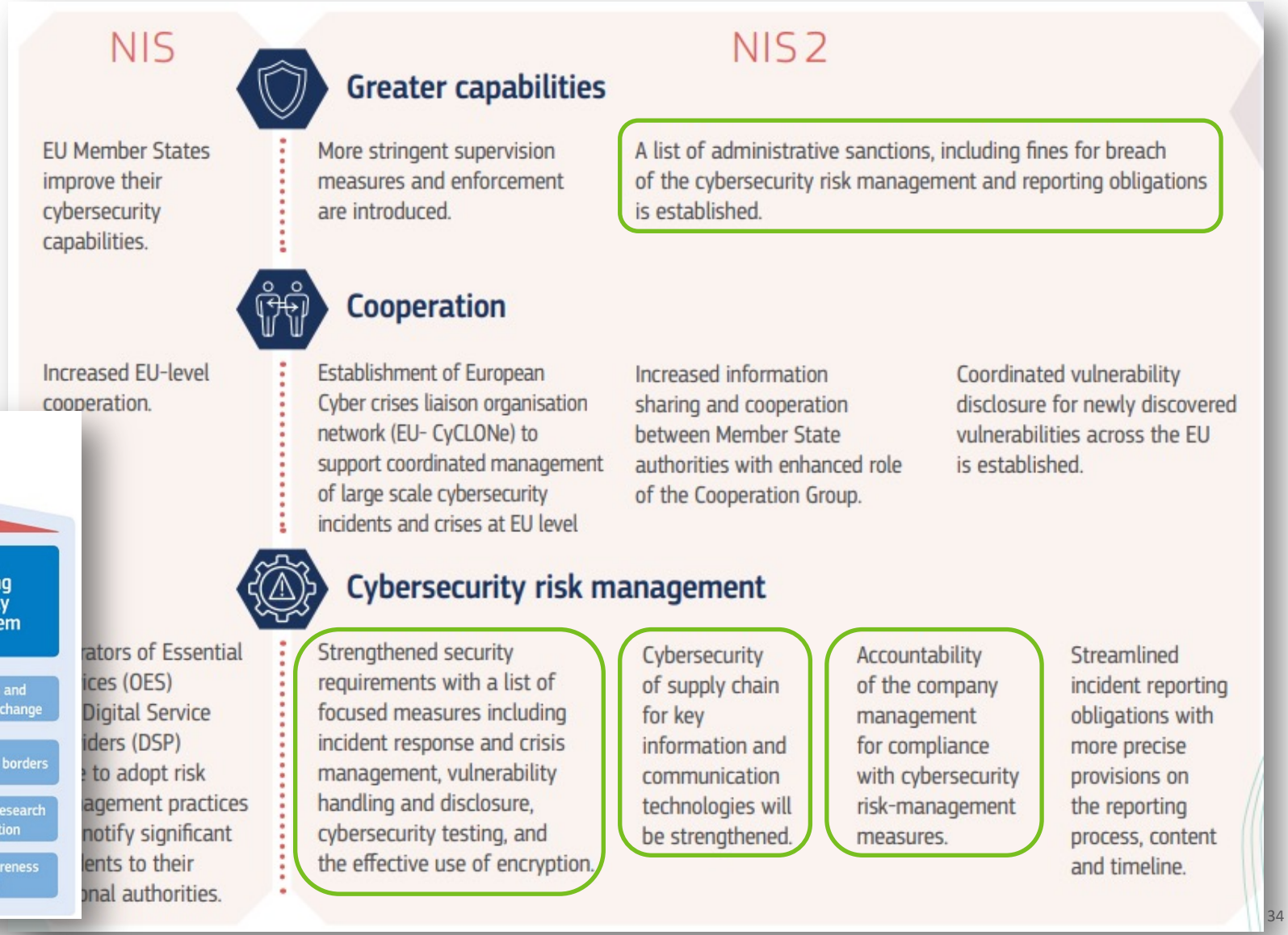
EU Supply Chain & DevSecOps & Incident/Vuln Reporting

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf

Technical:

- Enforcement of strong Authentication and Access Controls
- Establishes CVE and related standards & coordination agreements to other CVE-based registries
- Establishes top level DNS mandate
- Zero Trust – Priority 7 - ENISA

EU Security Union Strategy (European Commission, 2020b)



ZT Guidance

- NIST NCCoE ZTA Security Measures/Controls
- CISA Maturity Model
- CISA Cloud security Reference Architecture
- NIST and the EO Timeline (pacing of additional ZT standards and guidance)

NCCoE ZTA Security Control Map. Comparison and Audit of ZTAs

What's "Good Enough"? Pages 11-14

Cybersecurity Framework v1.1		
Function	**Category**	**Subcategory**
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried.
		ID.AM-2: Software platforms and applications within the organization are inventoried.
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented.
		ID.RA-3: Threats, both internal and external, are identified and documented.
PROTECT (PR)	Identity Management, Authentication, and Access Control (PR.AC)	PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
		PR.AC-3 Remote access is managed.
		PR.AC-4 Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.

+SBOM

Cybersecurity Framework v1.1		
Function	**Category**	**Subcategory**
		PR.AC-7 Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Data Security (PR.DS)	PR.DS-2 Data in transit is protected.
		PR.DS-5: Protections against data leaks are implemented.
		PR.DS-6 Integrity-checking mechanisms are used to verify software, firmware, and information integrity.
		PR.DS-8: Integrity-checking mechanisms are used to verify hardware integrity.
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of IT/industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).
		PR.IP-3: Configuration change control processes are in place.
	Protective Technology	PR.PT-3

Cybersecurity Framework v1.1		
Function	**Category**	**Subcategory**
DETECT	Anomalies and Events (DE.AE)	DE.AE-2: Detected events are analyzed to understand attack targets and methods.
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.
		DE.AE-5: Incident alert thresholds are established.
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.
		DE.CM-4: Malicious code is detected.
		DE.CM-5: Unauthorized mobile code is detected.
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.
		DE.CM-7 Monitoring for unauthorized personnel, connections, devices, and software is performed.
		DE.CM-8: Vulnerability scans are performed.
	Detection Processes (DE.DP)	DE.DP-5: Detection processes are continuously improved.
RESPOND	Mitigation (RS.MI)	RS.MI-1: Incidents are contained.
		RS.MI-2: Incidents are mitigated.

Multiple telemetry/sensor types collected and correlated (separation of Network, Endpoint, Service … telemetry/analytics is not the intent)

LP + LF
No single point of policy enforcement

Known Payload Ident Required

Known Vuln Ident Required

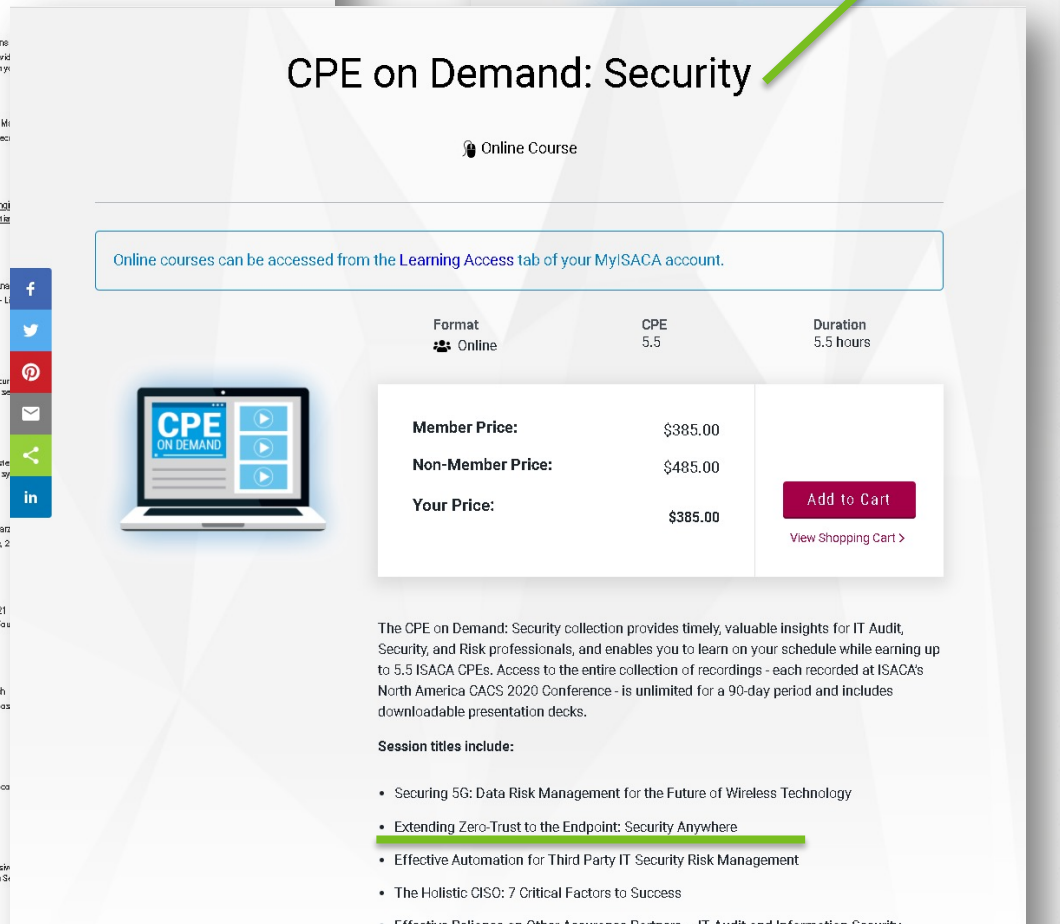
https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf

Granular Isolation

NSA: Container level at least.`

ZT Direction: ZT in Audit

200,000 Auditors : One ZT Definition



ZT Audit Prep - Global

Transform From Trust to Zero Trust at Asia CACS 2020

Author: ISACA
Date Published: 23 November 2020

This year, the COVID-19 pandemic and its resulting physical distancing requirements have made the idea of congregating with other professionals to explore industry topics and insights seem like a thing of the past. Yet the ISACA® community can still gather virtually to share insights and experiences through the online-only Asia CACS 2020 virtual conference. Asia CACS, taking place 11-12 December 2020, is designed to teach participants how to go from "Trust to Zero Trust."

The conference will have 3 parallel tracks available, exploring the following topics:

- **Track 1: Assurance**—The assurance path will include discussions about alignment to trust principles in safeguarding an organization, zero trust policy and its management, and how to audit a zero trust model.
- **Track 2: Defense**—This track will explore zero trust architecture, the role of microsegmentation in zero trust and access management in trust verification.
- **Track 3: Oversight**—The oversight track will focus on governance of the zero trust model, risk management in a zero trust framework and performance measurement in adherence with zero trust security vs. traditional security models.

Participants who attend can earn up to 14 continuing professional education (CPE) credits throughout the 2-day conference. An additional 7 CPE credits will be available to earn through the available pre-conference workshops.

To learn more about Asia CACS 2020 and register for the conference, visit the ISACA Asia CACS Conference page of the ISACA website.

CACS Global Auditor Guidance

Zero Trust Maturity Model

It is quite challenging to identify a maturity model for zero trust because there is no one size that fits all. Every organization is unique, operating in different industries with varied compliance requirements. As discussed, business priorities define the zero trust architecture and migration priorities. **Figure 4** shows the effort to develop a yard stick that generally satisfies the basic requirements. It provides indicative information that can be used for assessment.

Figure 4—Zero Trust Maturity Model

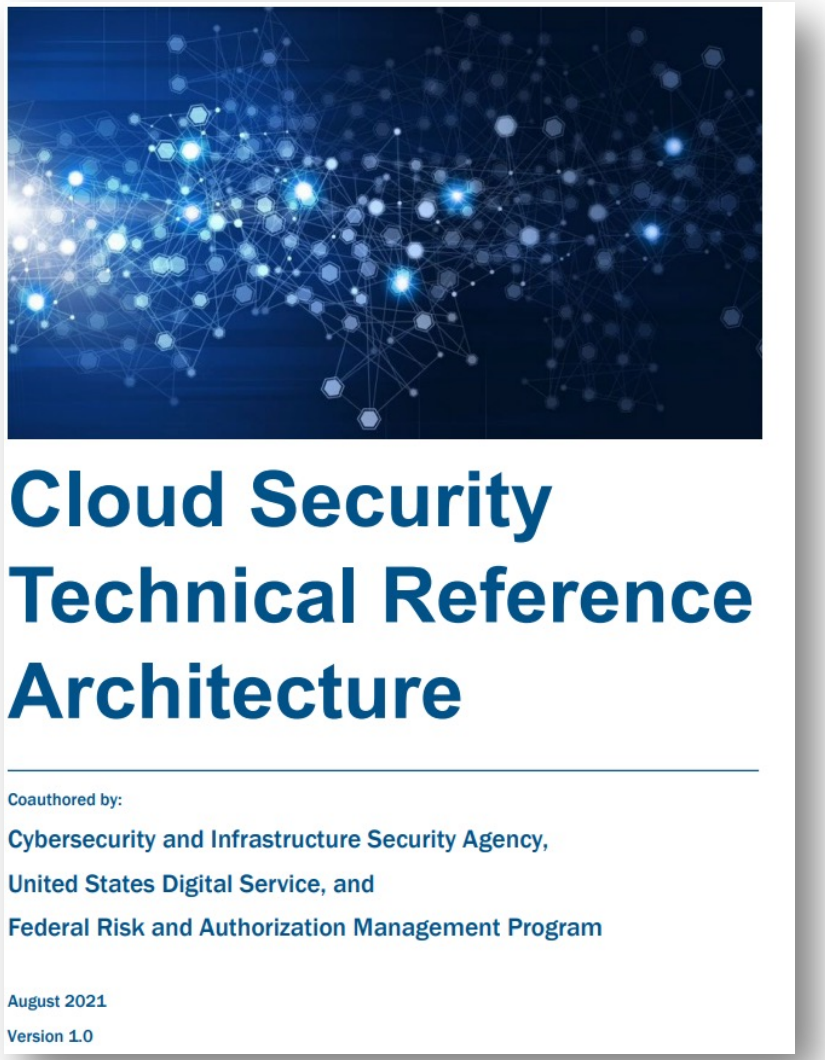
Zero Trust Elements	Initial	Developing	Defined	Managed	Optimizing
Data	Data sources and workflows are not formally documented. Access is granted on perimeter device controls.	Data sources, workflows and classification scheme are documented. Data are classified and labelled manually.	Automated content-based data classification, labelling and protection is in place.	ML for classification, labeling and protection is used. Data loss prevention (DLP) is governed by workflows and potential attack vectors.	Periodic review of ML algorithm configuration is undertaken to ensure alignment with business priorities.
Communication	No documented policy for securing communications. Network traffic is encrypted for outgoing with static traffic filtering.	Formal network security policy is in place. Traffic is encrypted, but not consistently applied. Servers and clients are in separate network segments.	All traffic is secured based on protect surface. Network segmentation is in place within the server's network segment. Logs are maintained and reviewed.	Logs are aggregated centrally and reviewed for trend analysis. Deeper dynamic microsegmentation is in place based on protect surface.	Continuous analytics through ML are used to identify attack vectors and improvements in network security.
User	Basic IAM, auditing at the system level and isolated single sign-on system (SSO) are used.	IAM with MFA, enterprise level SSO, auditing at system level with some integration to central logging repository are in place.	Automated IAM integrated with enterprisewide systems is in place, including session management, reauthentication, reauthorization and user activity logging	IAM integrated with other components such as device management, threat intel and mitigation, ML, and rapid incident response tools is used.	ML capability is used for session management based on various threat vectors. Periodically review reports from IAM and fine-tune IAM configurations and integration.
Devices	Devices are secured by antimalware, active directory group policies. Only authorized devices can connect to the enterprise network.	A device management tool is in place, which ensures a device's compliance with established policies before it is connected to the enterprise network.	Devices are protected through endpoint detection and response (EDR) technology with real-time threat intel and mitigation. Non-enterprise devices can connect to a separate network segment with limited Internet connectivity.	Access control is managed through the user and device compliance status. Continuous device monitoring for anomaly detection is used.	Proactive threat hunting, investigation and mitigation leveraged on ML and advanced analytics is employed.
Infrastructure	Manual processes for managing permissions across servers and virtual machines (VMs) are used. Applications are open to any authorized user in the network.	Automated privileged access management integrated with session workflow management is in place. User to application access is secured based on defined workflows. Cloud access security brokers (CASBs) are used.	Unauthorized deployments are identified and alerts are triggered. Workloads are monitored for anomalies. Every workload has an application tag.	User and resource sessions are tagged and continuously monitored. Applications are secured through least privileges, SSO and user sessions are continuously monitored.	Dynamic least privilege rules are coupled with AI to provide granular control across all workloads.

Zero Trust Adoption Trend

A 2020 zero trust progress report surveyed more than 400 cybersecurity decision-makers, ranging from technical executives to IT security practitioners and representing a balanced cross-section of organizations of varying sizes across multiple industries. According to one survey report, confidence among security professionals is mixed. Fifty-three percent have confidence, whereas 43 percent are still doubtful in applying a zero trust model in their architecture. This mixed reaction can be understood by the fact that 40 percent of zero trust implementations resulted in an increase in budget, whereas 45 percent of budgets remained the same, and only 15 percent of organizations witnessed a decrease in their budget. Seventy-two percent of organizations plan to assess or implement zero trust capabilities in some capacity in 2020 to mitigate growing cyberrisk.[11]

CISA Cloud Security Ref Arch (DRAFT - PC Opened 9/2021)

https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf



CISA CSRA Refers to Zero Trust 38 times:

"…

As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt zero trust architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with zero trust architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the FedRAMP within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

[…]

Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the Federal Civilian Executive Branch (FCEB), cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

…"

Zero Trust Extension

Implementing Zero Trust

Zero Trust – driving out implicit trust and reducing policy misconfiguration

- Assume compromise of … endpoint, host, supply chain, app, account, integrity -> continuous independent verification on granular isolation
- Establish the identity all subjects and continuously verify
- Assure confidentiality, Integrity, Availability of all objects and continuously verify
- Classify all interactions according to business risk
- ZT Reference Architectures Enable
  - logical colocation of intentional and observational controls
  - On boundaries logically close to subject to be protected and subjects to be controlled
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
  - https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/zta-project-description-final.pdf

– ZT Multi-Cloud: https://www.nist.gov/news-events/events/2021/01/devsecops-and-zero-trust-architecture-zta-multi-cloud-environments

– ZT Service Mesh: https://csrc.nist.gov/publications/detail/sp/800-204b/draft

SP 800-207

Zero Trust Architecture

Date Published: August 2020

Planning Note (12/11/2020): A Japanese translation of this publication was developed by PwC Consulting LLC for the Information-technology Promotion Agency (IPA), Japan.

Author(s)

Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (DHS)

Abstract

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

Keywords

architecture; cybersecurity; enterprise; network security; zero trust

SP 800-204B (Draft)

Attribute-based Access Control for Microservices-based Applications using a Service Mesh

Date Published: January 2021
Comments Due: February 24, 2021 (public comment period is CLOSED)
Email Questions to: sp800-204b-comments@nist.gov

Author(s)

Ramaswamy Chandramouli (NIST), Zack Butcher (Tetrate), Aradhna Chetal (TIAA)

Announcement

Deployment architecture in cloud-native applications now consists of loosely coupled components (microservices), with all application services provided through a dedicated infrastructure (service mesh) independent of the application code. Two critical security requirements in this architecture are (a) to build the concept of zero trust by enabling mutual authentication in communication between any pair of services and (b) a robust access control mechanism based on an access control model such as Attribute-based Access Control (ABAC) that can be used to express a wide set of policies and is scalable in terms of user base, objects (resources), and deployment environment.

The purpose of this document, Draft SP 800-204B, is to provide guidance for building an ABAC-based deployment within the service mesh that meets the requirements stated above. The security assurance provided by the deployment, the supporting infrastructure needed and the advantages of the Next Generation Access Control (NGAC), the ABAC model representation developed at NIST that is used in the deployment are also discussed.

NOTE: A call for patent claims is included on page iii of this draft. For additional information, see the Information Technology Laboratory (ITL) Patent Policy--Inclusion of Patents in ITL Publications.

DOCUMENTATION

Publication:
SP 800-204B (Draft) (DOI)
Local Download

Supplemental Material:
None available

Document History:
01/26/21: SP 800-204B (Draft)

TOPICS

Security and Privacy
access authorization; access control; authentication; zero trust

Technologies
cloud & virtualization

Recap

What is Zero Trust and how does it work (to address supply chain security, ransomware and complexity)?

Where are the standards now?

- NIST ZT Reference Architecture
- DoD ZT Reference Architecture
- NIST Guidance on ZT for Microservices and Service Mesh
- NCCoE Collaboration on ZT

The ZT Timeline

Guidance

- NIST NCCoE Audit Guidance
- CISA Maturity Model
- CISA Cloud security Reference Architecture
- Timeline (EO-14028, CMMC, EU NIS2, …)
- UK NCSC ZT Architecture Guidelines
- EU NIS2 ZT (ENISA) – Parlement vote in November

Thank You

Feedback, Questions, Followups and Collaboration

dmoreau@vmware.com

Appendix of Relevant Sources for ZTA Technical Requirements

From NIST bibliography on ZTA

NIST Cybersecurity Framework v.1.1, Framework for Improving Critical Infrastructure Cybersecurity
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
• NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments
https://doi.org/10.6028/NIST.SP.800-30r1
• NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach For Security and Privacy
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
• NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
• NIST SP 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
• NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf
• NIST SP 800-57 Part 1 Revision 4, Recommendation for Key Management: Part 1: General
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
• NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
• NIST SP 800-63 Revision 3, Digital Identity Guidelines
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
• NIST SP 800-92, Guide to Computer Security Log Management
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
• NIST SP 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
• NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf
• NIST SP 800-124 Revision 2 (Draft), Guidelines for Managing the Security of Mobile Devices in the Enterprise
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf
• NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach
https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
• NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
• NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf
• NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
• NIST SP 800-205, Attribute Considerations for Access Control Systems
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf
• NIST SP 800-207 (Second Draft), Zero Trust Architecture
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf
• NIST SP 1800-3, Attribute Based Access Control
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/abac-nist-sp1800-3-draft-v2.pdf
• Cloud Security Alliance, Software Defined Perimeter Working Group, SDP Specification 1.0
https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf
• ISO/IEC 27001, Information Technology–Security Techniques–Information Security Management Systems
• American Council for Technology-Industry Advisory Council, Zero Trust Cybersecurity Current Trends
https://www.actiac.org/system/files/ACTIAC%20Zero%20Trust%20Project%20Report%2004182019.pdf
• Federal Information Processing Standards 140-3, Security Requirements for Cryptographic Modules
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf